

(11)特許出願公開番号

特開平11-339045

(43)公開日 平成11年(1999)12月10日

(51) Int.Cl.<sup>6</sup>

識別記号

FI

G O 6 T 7/00

G O 6 F 15/62

465P

G O 6 F 17/60

15/21

**340B**

審査請求 未請求 請求項の数11 O.L (全 34 頁)

(21)出願番号 特願平10-145910

(22)出願日 平成10年(1998)5月27日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 田坂 光伸

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所システム開発本部内

(72)発明者 高橋 英男

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所システム開発本部内

(72) 發明者 増石 哲也

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所システム開発本部内

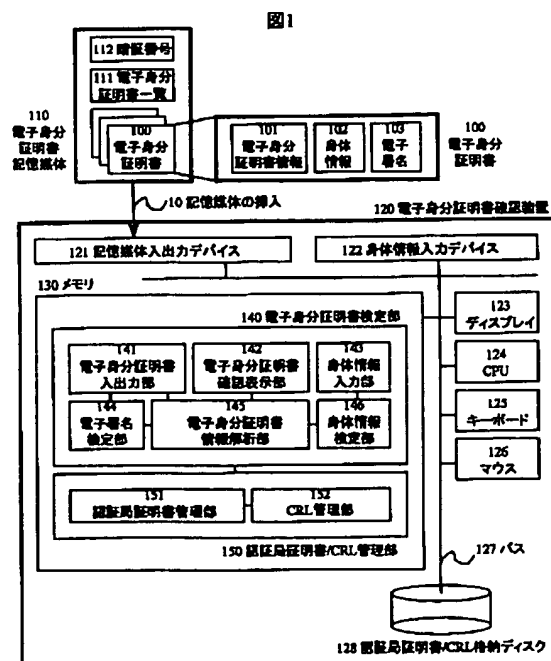
(74)代理人 弁理士 秋田 収喜

(54) 【発明の名称】 電子データ確認及び発行方法、その実施装置、その処理プログラムを記録した媒体並びに電子データ記録媒体

(57) 【要約】

【課題】 電子データ記録媒体に記録された電子データの不正使用を防止することが可能な技術を提供する。

【解決手段】 電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認方法において、電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定するステップと、当該電子データ記録媒体の保持者の身体情報を読み取り、読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定するステップとを有するものである。



## 【特許請求の範囲】

【請求項 1】 電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認方法において、

電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定するステップと、

当該電子データ記録媒体の保持者の身体情報を読み取り、読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定するステップとを有することを特徴とする電子データ確認方法。

【請求項 2】 前記身体情報に対する電子署名を検定するステップは、前記電子データの発行機関である電子データ認証局の暗号鍵を用いて前記電子データの所有者の身体情報に対する電子署名を検定するものであることを特徴とする請求項 1 に記載された電子データ確認方法。

【請求項 3】 前記身体情報に対する電子署名を検定するステップは、前記電子データの発行機関である電子データ認証局の暗号鍵に対する電子証明書が失効していないかを確認し、有効な電子証明書を用いて電子データ認証局の暗号鍵を検定し、前記検定が成功した暗号鍵を用いて前記身体情報に対する電子署名を検定するものであることを特徴とする請求項 1 に記載された電子データ確認方法。

【請求項 4】 前記電子データ認証局とは別の機関が作成した任意の電子データに対する電子署名を検定するステップを有することを特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載された電子データ確認方法。

【請求項 5】 電子データを記録した電子データ記録媒体を発行する電子データ発行方法において、電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取り、前記身体情報に対する電子署名を作成するステップと、前記電子データ、身体情報及びその電子署名を電子データ記録媒体に記録するステップとを備えることを特徴とする電子データ発行方法。

【請求項 6】 前記電子データの発行機関である電子データ認証局とは別の機関が作成した任意の電子データと、前記任意の電子データに対する電子署名とを前記電子データ記録媒体に追加するステップを有することを特徴とする請求項 5 に記載された電子データ発行方法。

【請求項 7】 電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認装置において、電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定する電子署名検定部と、

当該電子データ記録媒体の保持者の身体情報を読み取る

身体情報入力部と、前記身体情報入力部で読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定する身体情報検定部とを備えることを特徴とする電子データ確認装置。

【請求項 8】 電子データを記録した電子データ記録媒体を発行する電子データ発行装置において、電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取る身体情報入力部と、前記身体情報に対する電子署名を作成する電子署名作成部と、

前記電子データ、身体情報及びその電子署名を有するデータを作成する電子データ作成部と、前記電子データ作成部により作成したデータを電子データ記録媒体に記録する電子データ入出力部とを備えることを特徴とする電子データ発行装置。

【請求項 9】 電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認装置としてコンピュータを機能させる為のプログラムを記録した媒体において、

電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定する電子署名検定部と、

当該電子データ記録媒体の保持者の身体情報を読み取る身体情報入力部と、前記身体情報入力部で読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定する身体情報検定部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする媒体。

【請求項 10】 電子データを記録した電子データ記録媒体を発行する電子データ発行装置としてコンピュータを機能させる為のプログラムを記録した媒体において、電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取る身体情報入力部と、前記身体情報に対する電子署名を作成する電子署名作成部と、

前記電子データ、身体情報及びその電子署名を有するデータを作成する電子データ作成部と、前記電子データ作成部により作成したデータを電子データ記録媒体に記録する電子データ入出力部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする媒体。

【請求項 11】 特定の所有者が所有する電子データを記録した電子データ記録媒体において、その所有者が所有する電子データと、当該所有者の身体的特徴を示す身体情報と、当該身体情報の電子署名とを有するデータを記録したことを特徴とする電子データ記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は特定の人物に関する

情報を電子データとして発行し、その所有者の確認を行う電子データ処理システムに関し、特に人物の身分証明書をコンピュータが処理できる電子データとして実現し、当該身分証明書を発行したり、その保持者が所有者と一致するかを確認したりする電子データ処理システムに適用して有効な技術に関するものである。

#### 【0002】

【従来の技術】従来、身分証明書或いはそれに類似の個人情報情報を電子データとして実現することが広く行われている。なお本発明では、身分証明書の目的を以下の様に定義する。第一の目的は、身分証明書の保持者が身分証明書に記載された所有者本人であるかと、当該所有者が身分証明書の保証する資格を有していることを確認することである。第二の目的は、第一の目的事項の確認者が、身分証明書の保持者と対面している状態で、第一の目的事項を確認することである。

【0003】身分証明書或いはそれに類似の個人情報情報を電子データとして実現する従来の技術はいくつか存在しており、例えば第一の公知例としては、International Telecommunication Union発行の「ITU-T Recommendation X.509 (1997), Information Technology - Open Systems Interconnection - The Directory:Authentication Framework」に記載されている。

【0004】本公知例は、情報処理システムで用いられる暗号鍵の所有者が用いる電子証明書について記載しており、当該証明書は、証明書自体の識別番号、暗号鍵の所有者の名称、当該証明書の発行機関の名称、暗号鍵等の電子データと、その電子データに対する発行機関の電子署名とを格納している。

【0005】本公知例の電子証明書は、コンピュータネットワークにおいて電子的な商取引を行うためのシステムに適用されており、例えばクレジットカードによる支払いをコンピュータネットワークにおいて行うための通信手順を規定した「Secure Electronic Transaction Specification」(MasterCard International社及びVisa International社発行、1997)に述べられている様に、前記のデータのほか、郵便番号や住所等を示すデータを格納する。

【0006】本公知例の電子証明書の主な目的は、ある情報処理システムにおいて、送信者と受信者が、互いの暗号鍵を交換するときに、受け取った暗号鍵が確かに相手のものであるかと、相手が当該情報処理システムに参加する資格を有しているかを確認することである。

【0007】本公知例では、このような確認処理は、先に述べた「電子証明書の発行機関の電子署名」により実現される。電子署名は、暗号技術を用いた情報処理システムで広く用いられているもので、電子署名の対象データの改竄の防止と電子署名の作成者の認証を達成する。電子署名については、例えばPrentice Hall社発行の「Network Security」(1995)に記載されている。

【0008】電子署名は、本発明において重要な役割を果たすものであるので、ここで若干の説明を行う。

【0009】電子署名を実現する技術として公開鍵暗号技術が広く用いられている。公開鍵暗号では二つの暗号鍵が登場する。これを暗号鍵ペアと呼ぶ。暗号鍵ペアの一方は秘密鍵と呼ばれ、その暗号鍵ペアの所有者が秘匿の責任を負う。他方は公開鍵と呼ばれ、例えば情報処理システムにおける通信相手に渡すものである。

【0010】公開鍵暗号による電子署名は、以下の様に用いられる。以下では電子署名の作成者が、電子署名の検定者に渡したいデータのことを平文と呼ぶ。

【0011】先ず作成者は平文を秘密鍵で暗号化する。この平文を暗号化することにより生成されたデータを暗文と呼ぶ。この暗文が「電子署名」である。作成者は、平文と暗文（電子署名）を検定者に渡す。この平文と暗文の組合せを、以降、「電子署名データ」と呼ぶ。

【0012】次に検定者は、受け取った電子署名データの内、電子署名を作成者の公開鍵で復号する。作成者の公開鍵は、予め、または、電子署名データと共に、検定者に渡される。

【0013】次に検定者は、平文と電子署名を復号することにより得られたデータを比較する。以下では、この比較において、互いが一致することを検定の成功と呼び、一致しないことを検定の失敗と呼ぶ。

【0014】検定が成功したならば、以下のことがわかる。第一に、平文が改竄されていないことがわかる。平文を改竄すれば、電子署名の復号結果と一致しないからである。第二に、電子署名の作成者が、検定に用いた公開鍵と暗号鍵ペアを成す秘密鍵の所有者であることがわかる。何故なら、その公開鍵で復号できる暗文は、その公開鍵と暗号鍵ペアを成す秘密鍵で作成したものだけであることが、一般に公開鍵暗号アルゴリズムでは保証されているからである。

【0015】ここで、電子署名の作成者の公開鍵がすりかえられていると、検定の成功は、前記の二つの事項を保証しないことになってしまう。公開鍵のすりかえを検出する為に用いられるのが、まさに、第一の公知例の電子証明書である。第一の公知例の電子証明書は、例えば公開鍵の所有者の名称や公開鍵を平文の一部とする電子署名データであり、電子証明書の電子署名の検定を行うことにより、公開鍵を含めた証明書データの改竄が検出できる。なお、以降では、電子署名の対象データである平文のことを「電子署名対象データ」と呼ぶ。

【0016】第一の公知例の電子証明書は、その発行機関が、自らの秘密鍵により、電子証明書を含むデータに対して電子署名を施した電子署名データである。以下では、電子証明書の発行機関のことを認証局と呼ぶ。

【0017】電子証明書を受け取った者は、当該認証局の公開鍵を入手し、当該電子証明書の電子署名を検定する。以下では、電子証明書の電子署名の検定のことを、

単に「電子証明書の検定」と呼ぶ。電子証明書の検定により、当該電子証明書が含むデータが改竄されていないことと、当該電子証明書が当該認証局から発行されたものであることを確認できる。

【0018】ここで、電子証明書を検定する為に用いる認証局公開鍵がすりかわっていないことを保証する為に、更に電子証明書が用いられる。つまり、認証局の公開鍵は、電子証明書に格納されて配布される。第一の公知例では、認証局は階層的に構成されており、末端の暗号鍵所有者の電子証明書を発行する認証局自身の電子証明書は、更に上位の認証局が発行する。

【0019】なお、第一の公知例では、効力を失った電子証明書を示す電子データが用いられている。この電子データは、CRL(Certificate Revocation List)と呼ばれるもので、効力を失った電子証明書の一覧を示すデータである。以降では、電子証明書が効力を失うことを「失効」と呼ぶ。第一の公知例では、CRLは、末端の暗号鍵所有者の電子証明書の失効だけでなく、認証局の電子証明書の失効も管理する。

【0020】第二の公知例は、例えば特開平8-305766号公報「証明書自動交付機」に記載されている。本公知例は、住民票や印鑑証明書等の印刷物である証明書類の発行装置に関するもので、証明書の発行を申請する人が本人或いはその許可を得た人かどうかの確認を行うものである。本公知例では、ICカードに暗証番号と住民票や印鑑証明書等に記載されるべきデータを記憶する。証明書類の発行の際には、証明書自動交付機において、当該ICカードに記憶された暗証番号と発行申請者が入力する暗証番号を比較して本人確認を行う。

【0021】なお、本公知例では、ICカードに記憶された住民票や印鑑証明書等のデータは、証明書自動交付機が住民票や印鑑証明書等の印刷物である証明書類を作成する為に用いられる。本公知例では、身分証明書はICカードそのものであり、その保持者が当該ICカードに記憶されたデータを印刷した証明書類を発行する資格を有していることを保証する。

【0022】第三の公知例は、例えば特開平6-251049号公報「投票受付端末装置」に記載されている。本公知例は、選挙の投票受付端末装置に関するもので、投票を行う人(選挙人)が本人かどうかの確認を行うものである。本公知例では、選挙人が所有するICカードに当該選挙人の指紋の特徴データを記憶し、投票の際には、投票受付端末装置において当該ICカードに記憶された指紋と選挙人の指紋を比較して本人確認を行う。本公知例では、身分証明書はICカードそのものであり、その保持者が選挙権を有していることを保証する。

【0023】第四の公知例は、現在、広く用いられているカード型や手帳型の印刷された身分証明書であり、例えばパスポート、運転免許証、社員証、学生証等である。この様な身分証明書は、一般に、その所有者が、あ

る資格を有していることを保証し、それぞれの資格の審査機関が発行する。

【0024】

【発明が解決しようとする課題】人物が本人であるかと特定の資格を有しているかを確認する為の身分証明書を電子データとして実現しようとするとき、従来技術には以下の様な課題が存在する。

【0025】第一の公知例の電子証明書は、盗まれてしまった場合に、不正使用が可能であるという問題がある。電子証明書は、通常、ICカード等の記憶媒体に記憶され、第三の公知例にも登場している様に、記憶媒体の記憶領域へのアクセスが暗証番号により保護されると考えられる。しかし、他人に記憶媒体を盗まれ、かつ、暗証番号を知られてしまうと、当該電子証明書は読み出し可能になってしまう。

【0026】第一の公知例の電子証明書は認証局による電子署名データであり、当該電子証明書の検定者は、認証局の電子証明書を入手し、それが格納する認証局の公開鍵により、検定を行う。認証局電子証明書は、当該記憶媒体に格納されるか、検定者により、別途、入手されるものであるため、記憶媒体の暗証番号を看破されることにより、電子証明書の検定は成功してしまう。つまり、他人が盗んだ電子証明書の本人に成りすますことが可能になる。

【0027】そもそも、第一の公知例は、コンピュータネットワークでの電子商取引システム等の公開鍵暗号技術を用いて送受信するメッセージの保護を行う様な情報処理システムへの適用を狙ったものであり、公開鍵暗号技術と共に用いなければ効力を発揮しえない。つまり、第一の公知例を適用した情報処理システムでは、電子証明書自体は公開のものであり、悪意を持った他人が入手したとしても、電子証明書が格納する公開鍵と暗号鍵ペアを成す秘密鍵を入手しない限り、不正使用はできない。その様な情報処理システムでは、電子証明書は、データの暗号や電子署名の検定に用いられるが、これらが可能であったとしても、相対するデータの復号や電子署名の作成ができなければ意味がない。

【0028】第一の公知例を適用した情報処理システムでは、データの復号や電子署名の作成は、秘密鍵によってのみ行える様になっているので、第一の公知例の電子証明書は、それを適用した情報処理システムにおいては効力を発揮するのである。しかし、本発明が対象とする様な身分証明書としての使用は、第一の公知例の電子証明書が目的とするところではなく、効力を発揮しえない。

【0029】第二の公知例の身分証明書は、ICカード自体である。ICカード自体が、住民票等の印刷された証明書類を自動交付機で交付してもらう資格を示す身分証明書となっている。第二の公知例の身分証明書には、以下の二つの課題がある。第一の課題は、ICカード自体が身

分証明書となっているため、個人が有する資格毎に身分証明書が必要となり、その保持の為に多くのスペースを必要とするということである。第二の課題は、ICカードを盗まれた場合に、不正使用が可能であるということである。第二の公知例では、これを暗証番号により防御しようとしているが、暗証番号を知られてしまった場合には、防御できない。

【0030】第三の公知例の身分証明書は、ICカード自体である。ICカード自体が、選挙権を示す身分証明書になっている。第三の公知例には、以下の二つの課題がある。第一の課題は、ICカード自体が身分証明書となっているため、個人が有する資格毎に身分証明書が必要となり、その保持の為に多くのスペースを必要とするということである。第二の課題は、ICカードを盗まれた場合に、不正使用が可能であるということである。第三の公知例では、これを、当該ICカードの所有者の指紋データをICカードに格納し、当該指紋データをICカードの保持者の指紋と比較することにより防御しようとしている。しかし、ICカードを盗まれ、かつ、指紋データを偽造されてしまった場合には防御できない。また、同様のICカード自体を偽造することも可能と思われる。

【0031】第四の公知例の身分証明書には、以下の三つの課題が存在する。第一の課題は、個人が有する資格毎に身分証明書が必要となるため、その保持の為に多くのスペースを必要とするということである。第二の課題は、身分証明書を盗まれた場合に、写真や発行機関の印鑑等の偽造を行うことにより、不正使用が可能ということである。第三の課題は、身分証明書の確認者が、身分証明書の発行機関の確認する手間や時間がかかるということである。身分証明書の発行機関が確認者にとって未知のものであった場合、発行機関の存在やその信頼性を確認する為には、例えば身分証明書に記載されている発行機関の電話番号へ電話したり、役所等のしかるべき第三者機関へ問い合わせる等を行わねばならない。手間や時間がかかるが故に、この手続きがおろそかになる可能性は大きく、結果として、偽造された身分証明書の不正使用が可能になる。また、既知の発行機関であっても、当該発行機関の印鑑等の偽造を行うことにより、当該発行機関が発行する身分証明書自体の偽造が可能と思われる。

【0032】以上の様に、従来技術には、第一に身分証明書の携帯の為に多くのスペースを必要とすること、第二に身分証明書の不正使用が可能であること、第三に身分証明書の発行機関の信頼性の確認方法が確立されていない為に身分証明書の偽造が可能であること、といった課題がある。

【0033】本発明の目的は上記問題を解決し、電子データ記録媒体に記録された電子データの不正使用を防止することが可能な技術を提供することにある。

【0034】

【課題を解決するための手段】本発明は、電子データを記録した電子データ記録媒体を発行し、その所有者を確認する電子データ発行/確認方法において、当該電子データの所有者の身体情報及びその電子署名を有する電子データ記録媒体を発行し、その電子署名を検定して当該電子データの所有者を確認するものである。

【0035】本発明では、例えば電子データを電子身分証明書情報とし、電子データ記録媒体を電子身分証明書記憶媒体とし、電子データの発行機関である電子データ認証局を電子身分証明書認証局として、電子身分証明書情報を記録したICカード等の電子身分証明書記憶媒体を発行する場合、まず電子身分証明書の所有者となる人物の身体的特徴を示す身体情報を入力する。

【0036】次に前記入力した身体情報を電子身分証明書の発行機関である電子身分証明書認証局の暗号鍵で暗号化して当該身体情報に対する電子署名を作成した後、当該電子身分証明書の所有者の身体情報、前記作成した身体情報及びその電子署名を含む電子身分証明書を電子身分証明書記憶媒体に書き込む。

【0037】電子身分証明書記憶媒体の保持者が電子身分証明書の所有者であるかどうかを確認する場合には、電子身分証明書中の身体情報に対する電子署名を検定し、前記身体情報の検定が成功した場合に、電子身分証明書記憶媒体の保持者の身体情報を読み取り、その読み取った身体情報が前記電子身分証明書の身体情報と一致するかどうかを検定する。

【0038】本発明によれば、ある人物の身元や特定の資格を有しているかを確認する為の身分証明書等の各種情報を電子データとして実現できるので、単一の記録媒体に複数の身分証明書等の情報を格納することができ、複数の身分証明書の携帯に必要なスペースを削減することができる。

【0039】また、本発明によれば、電子身分証明書にその所有者の身体情報とその身体情報に対する電子署名を含め、当該電子身分証明書の確認を行う際に、前記の所有者の身体情報に対する電子署名を検定し、当該電子身分証明書を保持する者の身体的特徴と前記の所有者の身体情報を比較することにより、当該電子身分証明書を保持する者が当該電子身分証明書の所有者であるかを確認することができる。たとえ、前記の電子身分証明書の所有者の身体情報が改竄されていたとしても、前記の所有者の身体情報に対する電子署名を検定することによりこれを検出することができるので、当該身分証明書の不正使用を防止することができる。

【0040】また、本発明によれば、電子身分証明書の所有者の身体情報に対する電子署名を、電子身分証明書認証局がその暗号鍵を用いて作成した電子署名とすることができる。ここで、本発明によれば、電子身分証明書確認装置が、電子身分証明書認証局の暗号鍵の電子証明書である暗号鍵証明書を格納し、かつ、当該暗号鍵証明

書を検定できるので、電子身分証明書所有者の身体情報に対する電子署名を検定する為の暗号鍵を電子身分証明書認証局の暗号鍵証明書に含めて電子身分証明書確認装置へ配布することができ、かつ、前記の電子身分証明書認証局の暗号鍵証明書の電子署名を検定することで、前記の電子身分証明書認証局の信頼性及び前記の電子身分証明書認証局の暗号鍵の信頼性を確認することができる。

【0041】これにより、本発明によれば、電子身分証明書認証局の暗号鍵の偽造を防止することができ、電子身分証明書の偽造を防止することができる。また、電子身分証明書の確認者にとって未知の電子身分証明書認証局が発行したとされる電子身分証明書があったとしても、当該電子身分証明書認証局の信頼性を簡単に確認することができる。

【0042】以上の様に本発明の電子データ処理システムによれば、電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【0043】

【発明の実施の形態】（実施形態1）以下に所有者の身体的特徴を示す身体情報及びその電子署名により電子身分証明書の所有者を確認する実施形態1の電子データ処理システムについて説明する。

【0044】実施形態1は、電子身分証明書情報を電子データとして記録する電子身分証明書記憶媒体と、その所有者の確認を行う電子身分証明書確認装置の動作を説明するものである。図1から図11を用いて本実施形態を説明する。

【0045】図1は本実施形態の電子身分証明書のデータ構造、電子身分証明書を記憶する記憶媒体及び電子身分証明書確認装置の概略構成を示す図である。図1に示す様に本実施形態の電子身分証明書確認装置120は、電子身分証明書入出力部141と、電子身分証明書確認表示部142と、身体情報入力部143と、電子署名検定部144と、電子身分証明書情報解析部145と、身体情報検定部146と、認証局証明書管理部151と、CRL管理部152とを有している。

【0046】電子身分証明書入出力部141は記憶媒体入出力デバイス121を介して電子身分証明書記憶媒体110から、暗証番号112、電子身分証明書一覧111及び電子身分証明書100を読み取る処理部である。

【0047】電子身分証明書確認表示部142は電子身分証明書100の内容をディスプレイ123に表示する処理部である。身体情報入力部143は身体情報入力デバイス122を介して電子身分証明書記憶媒体110の保持者の身体情報102aを読み取る処理部である。

【0048】電子署名検定部144は電子身分証明書1

00の発行機関である電子身分証明書認証局の暗号鍵に対する暗号鍵証明書が失効していないかを確認し、有効な暗号鍵証明書を用いて電子身分証明書認証局の暗号鍵を検定し、前記検定が成功した暗号鍵を用いて、電子身分証明書記憶媒体110に記録された電子身分証明書100の電子身分証明書認証局電子署名103を検定する処理部である。

【0049】電子身分証明書情報解析部145は電子身分証明書100の電子身分証明書情報101を解析する処理部である。身体情報検定部146は身体情報入力部143で読み取った電子身分証明書記憶媒体110の保持者の身体情報102aが、電子身分証明書100の所有者の身体情報102と一致するかどうかを検定する処理部である。

【0050】認証局証明書管理部151は電子身分証明書100の電子身分証明書認証局電子署名103の検定に用いる電子身分証明書認証局の暗号鍵証明書を認証局証明書/CRL格納ディスク128を検索して取得する処理部である。CRL管理部152は失効した電子身分証明書100や、電子身分証明書認証局の暗号鍵証明書を示すCRLを管理する処理部である。

【0051】電子身分証明書確認装置120を電子身分証明書入出力部141、電子身分証明書確認表示部142、身体情報入力部143、電子署名検定部144、電子身分証明書情報解析部145、身体情報検定部146、認証局証明書管理部151及びCRL管理部152として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はCD-ROM以外の他の媒体でも良い。

【0052】電子身分証明書100は、電子身分証明書情報101、身体情報102及び電子身分証明書認証局電子署名103を含む電子データである。

【0053】電子身分証明書情報101は、当該電子身分証明書の所有者の氏名や所属等を示す身分情報や当該電子身分証明書の識別番号等の複数の電子データの集まりである。身体情報102は、当該電子身分証明書の所有者の身体的特徴を特定できるデータであり、例えば顔写真、指紋または声紋等を使用できる。また顔写真と身体的特徴を説明するテキストデータや、指紋と声紋等、複数の身体的特徴データを組合せたデータであっても良い。

【0054】電子身分証明書認証局電子署名103は、電子身分証明書情報101と身体情報102を組み合わせたデータを電子署名データとする電子署名である。電子身分証明書認証局電子署名103は、当該電子身分証明書の発行機関である電子身分証明書認証局が作成するものである。

【0055】電子身分証明書100の所有者は、当該電

子身分証明書を電子身分証明書記憶媒体110に格納して携帯する。電子身分証明書記憶媒体110は、複数の電子身分証明書100を格納しており、複数の電子身分証明書100は、それぞれ異なる電子身分証明書認証局が発行したものである。

【0056】ここで電子身分証明書記憶媒体110は、その所有者が所有する電子データである電子身分証明書情報101と、当該所有者の身体的特徴を示す身体情報102と、当該身体情報の電子身分証明書認証局電子署名103とを有するデータを記録したICカード等の電子データ記録媒体である。なお前記データを記録する記録媒体は、ICカード以外の他の媒体であっても良い。

【0057】また電子身分証明書記憶媒体110は、電子身分証明書一覧111と暗証番号112を格納している。電子身分証明書一覧111は、電子身分証明書記憶媒体110が格納している電子身分証明書100の一覧データある。暗証番号112は、電子身分証明書記憶媒体110から電子身分証明書100等を読み取る際にチェックに用いられるデータである。

【0058】電子身分証明書確認装置120は、電子身分証明書100を用いて、ある人物の資格を確認する為の装置である。以下では、電子身分証明書確認装置120を使用し、電子身分証明書100の保持者の資格を確認する人物のことを確認者と呼ぶ。また、ある時点で電子身分証明書100が格納された電子身分証明書記憶媒体110を携帯している人物のことを当該電子身分証明書の保持者と呼ぶ。電子身分証明書確認装置120は、電子身分証明書100の保持者が、確かに当該電子身分証明書の所有者であるかどうかという点と、確認者が確認したい資格を保有しているかどうかという点を確認する為の装置である。

【0059】電子身分証明書確認装置120は、以下の様な構造を有する。電子身分証明書確認装置120は、ディスプレイ123、CPU124、キーボード125、マウス126、メモリ130、バス127、記憶媒体入出力デバイス121、身体情報入力デバイス122、認証局証明書/CRL格納ディスク128から構成される。

【0060】メモリ130には、電子身分証明書検定部140及び認証局証明書/CRL管理部150というプログラムが存在する。記憶媒体入出力デバイス121は、電子身分証明書記憶媒体110が格納する電子データを読み取るデバイスである。身体情報入力デバイス122は、電子身分証明書100の保持者の身体情報102aを入力するデバイスであり、例えば指紋入力デバイスや声紋入力デバイス等を使用することができる。

【0061】電子身分証明書検定部140は、電子身分証明書100の保持者が当該電子身分証明書の所有者であるかを検定する。電子身分証明書入出力部141は、記憶媒体入出力デバイス121を介して、電子身分証明書記憶媒体110から、暗証番号112、電子身分証明

書一覧111、電子身分証明書100を読み取る。電子身分証明書確認表示部142は、電子身分証明書100の内容をディスプレイ123に表示する。

【0062】身体情報入力部143は、身体情報入力デバイス122を介して、電子身分証明書100の保持者の身体情報102aを読み取る。電子署名検定部144は、電子身分証明書100が失効していないかを確認し、電子身分証明書100の電子身分証明書認証局電子署名103を検定する。電子身分証明書情報解析部145は、電子身分証明書100の電子身分証明書情報101を解析する。身体情報検定部146は、身体情報入力部143が読み取った身体情報102aが、電子身分証明書100の身体情報102と一致するかどうかを検定する。

【0063】認証局証明書/CRL格納ディスク128は、電子身分証明書認証局の暗号鍵証明書やCRL等を格納する。なおここでは暗号鍵の電子証明書のことを「暗号鍵証明書」と呼んでいる。

【0064】認証局証明書/CRL管理部150は、電子身分証明書認証局の暗号鍵証明書やCRL等を管理する。認証局証明書管理部151は、電子身分証明書100の電子身分証明書認証局電子署名103の検定に用いる電子身分証明書認証局の暗号鍵証明書を認証局証明書/CRL格納ディスク128を検索して取得する。CRL管理部152は、CRLを認証局証明書/CRL格納ディスク128から検索する。電子身分証明書認証局の暗号鍵証明書とCRLについては、図2で詳しく説明する。

【0065】図2は本実施形態の電子データ処理システムのシステム構成を示す図である。本実施形態は、電子身分証明書確認装置120、電子身分証明書認証局203、統括認証局200から構成される。なお本実施形態において、複数の電子身分証明書確認装置120が存在しても良い。

【0066】電子身分証明書認証局203は、電子身分証明書100を発行する発行機関である電子データ認証局である。本実施形態では、電子身分証明書100の種類毎に複数の電子身分証明書認証局203が存在する。

【0067】統括認証局200は、電子身分証明書認証局203の暗号鍵証明書の発行機関であり、電子身分証明書認証局203の権威を保証する。また統括認証局200は、本実施形態で用いられる電子身分証明書100及び電子身分証明書認証局証明書182の内、失効したものの一覧であるCRL184の発行機関でもある。

【0068】電子身分証明書確認装置120の認証局証明書/CRL格納ディスク128には、電子身分証明書認証局証明書182、統括認証局公開鍵183、CRL184が格納される。

【0069】電子身分証明書認証局証明書182は、電子身分証明書認証局203の暗号鍵証明書である。統括認証局公開鍵183は、統括認証局200の公開鍵であ

る。CRL184は、失効した電子身分証明書100及び失効した電子身分証明書認証局証明書182の一覧情報である。

【0070】電子身分証明書認証局203は電子身分証明書認証局ディスク205を有する。電子身分証明書認証局ディスク205は、当該認証局の秘密鍵である電子身分証明書認証局秘密鍵204と、当該認証局の公開鍵の入った暗号鍵証明書である電子身分証明書認証局証明書182を格納している。

【0071】統括認証局200は、統括認証局ディスク202を有する。統括認証局ディスク202は、統括認証局200の秘密鍵である統括認証局秘密鍵201と、統括認証局200の公開鍵である統括認証局公開鍵183とCRL184を格納している。

【0072】本実施形態において、電子身分証明書確認装置120は、電子身分証明書認証局証明書182、CRL184、統括認証局公開鍵183を以下の様に入手する。

【0073】電子身分証明書認証局203は、統括認証局200から新たな電子身分証明書認証局証明書182を入手すると、任意の記憶媒体に電子身分証明書認証局証明書182を格納し、電子身分証明書確認装置120に送付する。

【0074】統括認証局200は、新たなCRL184を作成すると、任意の記憶媒体に当該CRL184を格納し、電子身分証明書確認装置120に送付する。また統括認証局200は、統括認証局公開鍵183を任意の記憶媒体に格納し、電子身分証明書確認装置120に送付する。

【0075】次に図3を用いて、本実施形態の電子身分証明書100及び電子身分証明書記憶媒体110の具体例を示す。

【0076】図3は本実施形態の電子身分証明書認証局203の概念を示す図である。図3は、人物A311及び人物B312が複数の電子身分証明書認証局203から電子身分証明書100の発行を受けている様子を示しており、本実施形態には、例えば電子身分証明書100として、自動車の運転免許証1001、パスポート1002やA大学学生証1004が存在する。

【0077】それぞれの電子身分証明書認証局203として、運転免許証発行機関2031、パスポート発行機関2032、A大学学生証発行機関2033が存在する。

【0078】人物A311は、自動車の運転資格と海外渡航資格を持っており、運転免許証発行機関2031から運転免許証1001を、パスポート発行機関2032からパスポート1002を、それぞれの発行機関において申請を行い発行してもらう(210)。

【0079】同様に人物B312は、海外渡航資格を持っており、A大学の学生である。そこで人物B312は、

パスポート発行機関2032からパスポート1003を、A大学学生証発行機関2033からA大学学生証1004を、それぞれの発行機関において申請を行って発行してもらう。

【0080】人物A311及び人物B312は、それぞれ自らの電子身分証明書記憶媒体A1101、電子身分証明書記憶媒体B1102に、複数の電子身分証明書100を格納して携帯する。ここで電子身分証明書確認装置120は、例えば出国審査機関に設置され、出国審査の際に電子身分証明書100であるパスポート1002を確認する為に用いられる。また電子身分証明書確認装置120は、例えば警察官によって携帯され、電子身分証明書100である運転免許証1001の確認の為に用いられる。

【0081】この様に本実施形態によれば、身分証明書を電子データとして実現でき、複数種類の電子身分証明書100を単一の電子身分証明書記憶媒体110に格納することができる。

【0082】次に図4を用いて本実施形態における電子身分証明書100、電子身分証明書認証局証明書182及びCRL184のデータ構造を説明する。

【0083】図4は本実施形態の電子身分証明書100、電子身分証明書認証局証明書182及びCRL184のデータ構造を示す図である。電子身分証明書100は、電子身分証明書情報101、身体情報102、電子身分証明書認証局電子署名103から構成される。

【0084】身体情報102については前述した。電子身分証明書認証局電子署名103は、電子身分証明書100の発行機関である電子身分証明書認証局203が作成する電子署名である。この電子署名の電子署名対象データは、電子身分証明書情報101と身体情報102からなる複合データである。

【0085】電子身分証明書情報101は、電子身分証明書ID1011、認証局証明書ID1012、身分情報1013から構成される。電子身分証明書ID1011は、電子身分証明書100に付与された一意な番号である。認証局証明書ID1012は、当該電子身分証明書を発行した電子身分証明書認証局203の暗号鍵証明書である電子身分証明書認証局証明書182の一意な番号である。身分情報1013は、電子身分証明書100の所有者の氏名、住所や所属等の身分を表す情報である。

【0086】電子身分証明書認証局証明書182は、認証局証明書ID1821、電子身分証明書認証局公開鍵1823、統括認証局電子署名1824から構成されている。認証局証明書ID1821は、電子身分証明書認証局証明書182を識別する一意な番号である。電子身分証明書認証局公開鍵1823は、電子身分証明書認証局証明書182の所有者である電子身分証明書認証局203の公開鍵である。統括認証局電子署名1824は、電子身分証明書認証局証明書182の発行機関である統括認



証局200が作成する電子署名である。この電子署名の電子署名対象データは、認証局証明書ID1821及び電子身分証明書認証局公開鍵1823から成る複合データである。

【0087】CRL184は、効力を失った電子身分証明書100及び電子身分証明書認証局証明書182の一覧データである。CRL184は、CRLID1841、電子身分証明書ID1842、認証局証明書ID1843、統括認証局電子署名1844から構成されている。

【0088】CRLID1841は、CRL184を識別する為の一意的な番号である。電子身分証明書ID1842は、失効した電子身分証明書100の一意的な番号であり、CRL184に複数エントリが存在する。認証局証明書ID1843は、失効した電子身分証明書認証局証明書182の一意的な番号であり、CRL184に複数エントリが存在する。統括認証局電子署名1844は、CRL184の発行機関である統括認証局200が作成する電子署名である。この電子署名の対象データは、CRLID1841、電子身分証明書ID1842、認証局証明書ID1843から成る複合データである。

【0089】次に、図5、図6、図7を用いて、本実施形態における電子身分証明書100及び電子身分証明書認証局証明書182の暗号技術を用いた確認の原理について説明する。これらの確認は電子署名を用いて行われるものである。本実施形態は、身体情報102と電子署名を併用することにより電子身分証明書100を実現するものであり、ここで説明する原理は本発明の根幹を成す。

【0090】先ず図5を用いて電子身分証明書100の電子身分証明書認証局電子署名103の作成に関する原理について説明する。

【0091】図5は本実施形態の電子身分証明書100の作成の原理を示す図である。電子署名対象データ501は、電子身分証明書認証局電子署名103を作成する際の対象データである。電子署名対象データ501は、電子身分証明書情報101及び身体情報102から成る。

【0092】電子身分証明書100は、電子身分証明書情報101及び身体情報102を電子署名対象データ501から複写し(502)、電子身分証明書認証局電子署名103との複合データとすることにより作成される。電子身分証明書認証局電子署名103は、電子署名対象データ501を、電子身分証明書認証局秘密鍵204により暗号化したものである(503)。

【0093】次に図6を用いて、電子身分証明書100の電子身分証明書認証局電子署名103の検定に関する原理について説明する。

【0094】図6は本実施形態の電子身分証明書100の確認の原理を示す図である。先ず、電子身分証明書100の電子身分証明書情報101及び身体情報102を

複写して電子署名対象データ601を作成する(602)。次に、電子身分証明書認証局電子署名103を電子身分証明書認証局公開鍵1823を用いて復号し、復号結果を電子署名対象データ601と比較して一致するかを調べる。この比較操作が、電子身分証明書認証局電子署名103の検定(603)である。

【0095】本実施形態において、この検定操作は電子身分証明書確認装置120において行われており、電子身分証明書確認装置120は、電子身分証明書認証局公開鍵1823を電子身分証明書認証局証明書182から抽出して入手する。これにより、電子身分証明書100の電子身分証明書情報101及び身体情報102に改竄がないことと、電子身分証明書100の発行元が電子身分証明書認証局証明書182の所有者である電子身分証明書認証局203であることを確認できる。

【0096】次に図7を用いて、電子身分証明書認証局証明書182の統括認証局電子署名1824の検定に関する原理について説明する。この統括認証局電子署名1824は、電子身分証明書認証局証明書182の発行機関である統括認証局200が、統括認証局秘密鍵201を用いて作成したものである。

【0097】図7は本実施形態の電子身分証明書認証局証明書182の確認の原理を示す図である。先ず、電子身分証明書認証局証明書182の認証局証明書ID1821及び電子身分証明書認証局公開鍵1823を複写して、電子署名対象データ701を作成する(702)。次に、統括認証局電子署名1824を統括認証局公開鍵183を用いて復号し、復号結果を電子署名対象データ701と比較して一致するかどうかを調べる。この比較操作が、統括認証局電子署名1824の検定(703)である。

【0098】本実施形態では、この検定操作は電子身分証明書確認装置120において行われる。これにより、電子身分証明書認証局証明書182の認証局証明書ID1821及び電子身分証明書認証局公開鍵1823に改竄がないことと、電子身分証明書認証局証明書182の発行元が統括認証局200であることを確認できる。

【0099】次に図8から図11を用いて、本実施形態における電子身分証明書確認装置120の動作の流れを説明する。

【0100】図8は本実施形態の電子身分証明書一覧111の概要を示す図である。電子身分証明書一覧111は、電子身分証明書記憶媒体110に格納されている電子身分証明書100の一覧である。電子身分証明書一覧111は、電子身分証明書100のそれぞれに対応するエントリを有する。それぞれのエントリは、電子身分証明書ID1011、電子身分証明書種別802、電子身分証明書認証局名804から構成される。電子身分証明書ID1011は、当該電子身分証明書を識別する為の一意的な番号である。電子身分証明書種別802は、当該電子

身分証明書がどのような種類の身分証明書であるかを示す。電子身分証明書認証局名804は、当該電子身分証明書を発行した電子身分証明書認証局203の名称である。

【0101】次に図9を用いて、電子身分証明書確認装置120が電子身分証明書100の確認を行う動作の流れを説明する。

【0102】図9は本実施形態の電子身分証明書確認装置120が電子身分証明書100の確認を行う処理の処理手順を示すフローチャートである。まず、電子身分証明書100の保持者は、電子身分証明書記憶媒体110を記憶媒体入出力デバイス121に挿入する(902)。次に電子身分証明書100の保持者は、キーボード125を介して電子身分証明書記憶媒体110の暗証番号112aを入力する(904)。これは、電子身分証明書確認装置120が、電子身分証明書記憶媒体110の保持者がその所有者かどうかを確認するためである。

【0103】電子身分証明書検定部140は、これを受けて、入力された暗証番号112aと電子身分証明書記憶媒体110の暗証番号112を比較する(906)。一致しなければ、電子身分証明書検定部140はディスプレイ123に電子身分証明書100の確認が失敗したことを表示する(918)。一致すれば、電子身分証明書検定部140は、電子身分証明書一覧111の内容をディスプレイ123に表示する(908)。

【0104】次に確認者は、確認対象の電子身分証明書100を選択し、それをキーボード125或いはマウス126を介して入力する(909)。次に電子身分証明書検定部140は、選択された電子身分証明書100を電子身分証明書記憶媒体110から読み込み、電子身分証明書認証局電子署名103を検定する(910)。

【0105】検定が失敗すると、電子身分証明書検定部140はディスプレイ123に電子身分証明書100の確認が失敗したことを表示する(918)。検定が成功すれば、電子身分証明書検定部140は、電子身分証明書100の身分情報1013と身体情報102を抽出する(911)。検定が成功したことにより、電子身分証明書100の電子身分証明書情報101の内容と身体情報102には改竄が無く、電子身分証明書認証局203が保証する内容が格納されていることが確認されたことになる。

【0106】次に電子身分証明書100の保持者は、身体情報入力デバイス122を介して身体情報102aを入力する(912)。例えば身体情報102として指紋が用いられる場合には指紋を、声紋が用いられる場合には声紋を入力する。

【0107】次に電子身分証明書検定部140は、入力された身体情報102aと電子身分証明書100の身体情報102を比較する(914)。一致しなければ、電

子身分証明書検定部140はディスプレイ123に電子身分証明書100の確認が失敗したことを表示する(918)。一致すれば、電子身分証明書検定部140は、ディスプレイ123に電子身分証明書100の確認が成功したことを、身分情報1013の内容を表示する(916)。

【0108】身体情報102が入力された身体情報102aと一致したことにより、電子身分証明書100の保持者が、確かにその所有者であることが確認されたことになる。最後に確認者は、ディスプレイ123に表示された身分情報1013の内容が、自分の要求する資格を満たしているものかどうかを確認することになる。

【0109】ここで電子身分証明書記憶媒体110が、正式な所有者ではない他の人物Cにより保持されており、人物Cが暗証番号112を知ることができたという状況を考える。このような場合であっても、本実施形態の電子身分証明書確認装置120は、人物Cが電子身分証明書100の所有者でないことを検出することができる。この場合、ステップ906において、入力された暗証番号112aと暗証番号112の比較は一致する。しかし、ステップ914において、入力された身体情報102aと身体情報102の比較が失敗するため、電子身分証明書100の確認は失敗する。

【0110】次に、電子身分証明書記憶媒体110が、正式な所有者ではない他の人物Cにより保持されており、人物Cが暗証番号112を知ることができ、かつ、人物Cが電子身分証明書100の身体情報102を自分の身体情報102aに入れ替えたという状況を考える。このような場合であっても、本実施形態の電子身分証明書確認装置120は、人物Cが電子身分証明書100の所有者でないことを検出することができる。

【0111】この場合、ステップ906において、入力された暗証番号112aと暗証番号112の比較は成功する。また、ステップ914まで進んだとすると、入力された身体情報102aと身体情報102の比較は成功してしまう。しかし、この場合には、ステップ910において、電子身分証明書100の電子身分証明書認証局電子署名103の検定が失敗する。何故なら、図6で説明した通り、人物Cの入れ替えた身体情報102aが電子身分証明書100の発行の際の電子身分証明書認証局電子署名103の作成に用いた身体情報102と異なっていると、電子署名検定(603)が失敗するからである。これにより、電子身分証明書100の確認が失敗する。

【0112】この様に本実施形態によれば、電子身分証明書100が他人により使用されたとしても、電子身分証明書確認装置120に入力された身体情報102aと電子身分証明書100の身体情報102を比較することにより、その事実を検出することができる。また、電子身分証明書100の身体情報102が改竄されていたと

しても、電子身分証明書認証局電子署名103の検定により、その事実を検出することができる。

【0113】なお本実施形態では、身体情報検定部146が、電子身分証明書100の身体情報102を、身体情報入力デバイス122を介して入力された電子身分証明書100の保持者の身体情報102aと比較する様にしたが、電子身分証明書確認表示部142が電子身分証明書100の身体情報102の内容をディスプレイ123に表示し、確認者が前記のディスプレイ123に表示された内容を電子身分証明書100の保持者の身体情報102aと比較する様にしても良い。

【0114】次に図10を用いて、図9のステップ910の動作を詳しく説明する。図10は本実施形態の電子身分証明書100の確認装置の動作の内、電子身分証明書100の電子身分証明書認証局電子署名103の検定処理の処理手順を示すフローチャートである。ステップ910は、電子身分証明書検定部140が電子身分証明書100の電子身分証明書認証局電子署名103の検定を行うものである。

【0115】電子身分証明書検定部140において、電子身分証明書入出力部141は、電子身分証明書100を電子身分証明書記憶媒体110から読み取り、電子署名検定部144にその検定を要求する(9102)。

【0116】次に電子署名検定部144は、電子身分証明書100の電子身分証明書情報101から認証局証明書ID1012を調べる(9104)。次に電子署名検定部144は、ステップ9104で読み出した認証局証明書ID1012を有する電子身分証明書認証局証明書182とCRL184を認証局証明書/CRL管理部150へ要求する(9106)。

【0117】認証局証明書/CRL管理部150は、電子署名検定部144から要求された電子身分証明書認証局証明書182とCRL184を検索する(9108)。本実施形態では、ステップ9108の動作は、認証局証明書/CRL格納ディスク128から電子身分証明書認証局証明書182とCRL184の検索として行われる。

【0118】ステップ9108で検索が失敗すると、電子署名検定部144は電子身分証明書入出力部141に検定失敗を応答する(914)。検索が成功すると、電子署名検定部144は、電子身分証明書100の電子身分証明書ID1011がCRL184に記載されていないかを検査する(9109)。

【0119】記載があると、その電子身分証明書100が失効しているということなので、電子署名検定部144は電子身分証明書入出力部141に検定失敗を応答する(9114)。記載がないと、電子署名検定部144は、電子身分証明書認証局証明書182の電子身分証明書認証局公開鍵1823を用いて、電子身分証明書100の電子身分証明書認証局電子署名103を検定する(9110)。この手順の原理は、図6で説明した通り

である。

【0120】検定が失敗すると、電子署名検定部144は電子身分証明書入出力部141に検定失敗を応答する(9112)。検定が成功すると、電子署名検定部144は電子身分証明書入出力部141に検定成功を応答する(9114)。なお、本実施形態において、電子身分証明書100に有効期限を示すデータを設け、ステップ910の動作において有効期限を検査する様にしても良い。

10 【0121】次に図11を用いて、電子身分証明書確認装置120が、電子身分証明書認証局証明書182とCRL184を入手する際の動作について述べる。

【0122】図11は本実施形態の電子身分証明書確認装置120が電子身分証明書認証局証明書182とCRL184を入手する処理の処理手順を示すフローチャートである。図2の説明で述べた通り、電子身分証明書認証局203は、電子身分証明書認証局証明書182が更新されると、新たな電子身分証明書認証局証明書182を任意の記憶媒体に格納して電子身分証明書確認装置120へ送付する。

20 【0123】また統括認証局200は、CRL184が更新されると、新たなCRL184を任意の記憶媒体に格納して電子身分証明書確認装置120へ送付する。ここで認証局証明書/CRL管理部150は、電子身分証明書認証局証明書182及びCRL184を前記の記憶媒体から入力する。

30 【0124】認証局証明書/CRL管理部150において、認証局証明書管理部151は、統括認証局公開鍵183を用いて電子身分証明書認証局証明書182の統括認証局電子署名1824を検定する(1104)。

【0125】ステップ1104の電子署名の検定の原理は、図7で説明した通りである。検定が失敗すると動作を終了する。検定が成功すると認証局証明書管理部151は、電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスク128に格納する(1106)。

40 【0126】次にCRL管理部152は、認証局証明書/CRL格納ディスク128に格納されている統括認証局公開鍵183を用いて、CRL184の統括認証局電子署名1844を検定する(1108)。検定が失敗すると動作を終了する。検定が成功するとCRL管理部152は、CRL184を認証局証明書/CRL格納ディスク128に格納する(1110)。

50 【0127】次にCRL管理部152は、認証局証明書/CRL格納ディスク128に格納されている電子身分証明書認証局証明書182の認証局証明書ID1821が、CRL184に記載されているかを検査する(1112)。記載がなければ終了する。記載があれば、CRL管理部152は、CRL184に記載のあった電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスク128から消去する(1114)。

【0128】この様に本実施形態では、図11のステップ1104において、電子身分証明書認証局証明書182の統括認証局電子署名1824の検定が成功すれば、電子身分証明書100の電子身分証明書認証局203が、確かな電子身分証明書100の発行機関であると保証されていることがわかる。

【0129】電子身分証明書認証局証明書182は、ステップ1104の統括認証局電子署名1824の検定が成功しないかぎり、認証局証明書/CRL格納ディスク128には格納されえない。よって、確認者は、電子身分証明書確認装置120により電子身分証明書100を確認する動作を行っている際、図10のステップ9108において、電子身分証明書認証局証明書182の検索の成否により、電子身分証明書認証局203の権威が保証されているかどうかを知ることができる。

【0130】また逆に、統括認証局200の認定を得ていない発行機関は、統括認証局電子署名1824の入った電子身分証明書認証局証明書182を所有することができない。よって、統括認証局200の認定を得ていない発行機関が発行した電子身分証明書100の保持者が現れたとしても、電子身分証明書確認装置120は、予め図11のステップ1104において電子身分証明書認証局証明書182の統括認証局電子署名1824を検定することにより、その様な発行機関の電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスク128から排除できるので、電子身分証明書100が有効なものでないことを検出することができる。

【0131】この様に本実施形態によれば、電子身分証明書認証局証明書182を検定することにより、電子身分証明書認証局203の権威が保証されていることを簡単に確認することができる。また電子身分証明書認証局証明書182を検定することにより、電子身分証明書認証局証明書182及びそれが含む電子身分証明書認証局公開鍵1823が偽造されたことを検出できるので、電子身分証明書100が偽造されていることを検出できる。

【0132】また本実施形態では、電子身分証明書確認装置120は、図10のステップ9109により、電子身分証明書100の発行後に資格が停止された人物の電子身分証明書100や、電子身分証明書記憶媒体110の紛失時に当該電子身分証明書記憶媒体に格納されている電子身分証明書100を、CRL184を用いて拒否することができる。

【0133】この様に本実施形態によれば、資格が停止された人物の電子身分証明書100や紛失してしまった電子身分証明書100を失効させ、その様な電子身分証明書100の確認が成功してしまうことを防止することができる。

【0134】以上説明した様に本実施形態の電子データ処理システムによれば、電子データ記録媒体に記録され

た電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【0135】（実施形態2）以下に電子身分証明書認証局証明書を通信ネットワークを介して入手する実施形態2の電子データ処理システムについて説明する。

【0136】実施形態1では、電子身分証明書確認装置120が電子身分証明書100の確認の為の動作を行う際、電子身分証明書認証局203の電子身分証明書認証局証明書182は、予め認証局証明書/CRL格納ディスク128に格納されていた。

【0137】これに対して本実施形態では、電子身分証明書確認装置120が電子身分証明書100の確認の為の動作を行う際、認証局証明書/CRL格納ディスク128に電子身分証明書認証局203の電子身分証明書認証局証明書182が無ければ、通信ネットワークを介して電子身分証明書認証局証明書182を入手する。

【0138】図12は本実施形態の電子身分証明書100のデータ構造、電子身分証明書100を記憶する記憶媒体及びその確認装置の概要を示す図である。電子身分証明書100、電子身分証明書記憶媒体110の構造は、実施形態1と同一である。電子身分証明書確認装置120は、電子身分証明書100を確認する為の装置であり、実施形態1の電子身分証明書確認装置120とほぼ同一の構造を有する。以下、主に実施形態1と異なる点について説明する。

【0139】電子身分証明書確認装置120において、電子身分証明書検定部140は、実施形態1と同様の構造を有し同様に動作する。認証局証明書/CRL格納ディスク128は、実施形態1と同様に電子身分証明書認証局証明書182、統括認証局公開鍵183、CRL184を格納する。認証局証明書/CRL管理部150は、電子身分証明書認証局証明書182、CRL184を管理する。認証局証明書/CRL管理部150は、実施形態1とは異なり、認証局証明書管理サーバアクセス部153を有し、実施形態1と異なる動作を行うが、電子身分証明書検定部140との接続形態は実施形態1と同様である。

【0140】電子身分証明書確認装置120は、通信ネットワークコントローラ160を有し、通信ネットワーク170を介して認証局証明書管理サーバ180と接続されている。通信ネットワーク170は、有線ネットワークでも無線ネットワークでも良い。

【0141】認証局証明書管理サーバ180は、電子身分証明書認証局証明書182、CRL184を管理する。認証局証明書管理サーバ180は、認証局証明書管理サーバディスク181を持つ。認証局証明書管理サーバディスク181は、電子身分証明書認証局証明書182、CRL184を格納する。

【0142】認証局証明書/CRL管理部150において、

認証局証明書管理部151は、電子身分証明書認証局203の電子身分証明書認証局証明書182を取得する。電子身分証明書認証局証明書182は、認証局証明書/CRL格納ディスク128を検索して取得されるか、或いは、認証局証明書管理サーバ180から取得されるか、或いは、取得できないかのいずれかである。CRL管理部152は、CRL184を認証局証明書/CRL格納ディスク128から検索する。

【0143】認証局証明書管理サーバアクセス部153は、認証局証明書管理サーバ180へ、通信ネットワーク170を介して、電子身分証明書認証局証明書182を要求する。認証局証明書管理サーバ180は、認証局証明書管理サーバディスク181を検索して、目的の電子身分証明書認証局証明書182があれば、それを通信ネットワーク170を介して返す。

【0144】図13は本実施形態の電子データ処理システムのシステム構成を示す図である。通信ネットワーク170に、電子身分証明書確認装置1200、認証局証明書管理サーバ180、電子身分証明書認証局203、統括認証局200が接続されている。本実施形態では電子身分証明書100の種類毎に複数の電子身分証明書認証局203が存在する。また本実施形態において、複数の電子身分証明書確認装置1200が存在しても良い。

【0145】認証局証明書管理サーバ180は、電子身分証明書認証局証明書182、統括認証局公開鍵183、CRL184を、認証局証明書管理サーバディスク181に格納し、電子身分証明書確認装置1200に供給する。

【0146】電子身分証明書認証局203は、統括認証局200から新たな電子身分証明書認証局証明書182を取得すると、電子身分証明書認証局証明書182を認証局証明書管理サーバ180に通信ネットワーク170を介して渡す。認証局証明書管理サーバ180は、渡された電子身分証明書認証局証明書182を認証局証明書管理サーバディスク181に格納しておく。

【0147】また統括認証局200は、CRL184が更新されると、それを、認証局証明書管理サーバ180に通信ネットワーク170を介して渡す。認証局証明書管理サーバ180は、渡されたCRL184を認証局証明書管理サーバディスク181に格納しておく。なお本実施形態において、複数の認証局証明書管理サーバ180を、例えば地域毎に設置しても構わない。

【0148】本実施形態において電子身分証明書確認装置1200は、電子身分証明書認証局証明書182、CRL184、統括認証局公開鍵183を以下の様に入手する。

【0149】電子身分証明書確認装置1200は、電子身分証明書100の確認に必要な電子身分証明書認証局証明書182を通信ネットワーク170を介して認証局証明書管理サーバ180から入手する。

【0150】認証局証明書管理サーバ180は、新たなCRL184を入手すると、通信ネットワーク170を介して電子身分証明書確認装置1200に送付する。また統括認証局200は、統括認証局公開鍵183を任意の記憶媒体に格納し、電子身分証明書確認装置1200に送付する。

【0151】次に図14を用いて、本実施形態における電子身分証明書確認装置1200の動作の流れを説明する。本実施形態において、電子身分証明書確認装置1200の動作は、実施形態1の図9、図10で説明した電子身分証明書確認装置120の動作と同様である。但し本実施形態においては、図10のステップ9108の動作が実施形態1とは異なる。図14は、本実施形態でのステップ9108の動作の詳細を説明するものである。

【0152】図14は本実施形態の電子身分証明書確認装置1200の処理手順を示すフローチャートである。ステップ9108で、認証局証明書/CRL管理部150は、電子身分証明書100の電子身分証明書認証局電子署名103の検定を行う際に用いる電子身分証明書認証局証明書182とCRL184を検索する。すなわち認証局証明書/CRL管理部150において、認証局証明書管理部151は、統括認証局公開鍵183とCRL184を、認証局証明書/CRL格納ディスク128から検索する(1402)。

【0153】次に、認証局証明書管理部151は、認証局証明書/CRL格納ディスク128から、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を検索する(1404)。検索が成功すると、認証局証明書管理部151は、電子身分証明書認証局証明書182とCRL184を電子署名検定部144に返す(1418)。検索が失敗すると、認証局証明書管理部151は、認証局証明書管理サーバアクセス部153へ、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を要求する(1406)。

【0154】次に、認証局証明書管理サーバアクセス部153は、通信ネットワークコントローラ160、通信ネットワーク170を介して、認証局証明書管理サーバ180に、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を要求する(1408)。

【0155】次に、認証局証明書管理サーバ180は、認証局証明書管理サーバディスク181から、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を検索する。検索成功なら電子身分証明書認証局証明書182を、認証局証明書管理サーバアクセス部153に返し、検索失敗ならその旨を示す応答を返す(1410)。検索失敗なら、認証局証明書管理部151は、検索失敗を示す応答を電子署名検定部144に返す(1420)。

【0156】検索成功であれば、認証局証明書管理部151は、電子身分証明書認証局証明書182の認証局証

明書ID1821がCRL184に記載されていないかを検査する(1412)。

【0157】記載がある場合には、認証局証明書管理部151は、検索失敗を示す応答を電子署名検定部144に返す(1420)。この場合、電子身分証明書認証局証明書182が失効していることになり、当該証明書の電子身分証明書認証局公開鍵1823により検定される電子身分証明書100を有効でないとみなす。

【0158】ステップ1412で記載がない場合には、認証局証明書管理部151は、統括認証局公開鍵183を用いて、電子身分証明書認証局証明書182の統括認証局電子署名1824を検定する(1414)。この動作は、図7で説明した原理を用いて行われる。

【0159】検定失敗であれば、認証局証明書管理部151は、検索失敗を示す応答を電子署名検定部144に返す(1420)。検定成功であれば、認証局証明書管理部151は、電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスク128に格納し(1416)、認証局証明書管理部151が電子身分証明書認証局証明書182とCRL184を電子署名検定部144に

返す(1418)。

【0160】なお、本実施形態において、電子身分証明書確認装置1200がCRL184を入手したときの動作は、実施形態1の図11のステップ1108からステップ1114と同様に実施できる。

【0161】この様に本実施形態によれば、電子身分証明書確認装置1200は、電子身分証明書認証局203の電子身分証明書認証局証明書182を必要になったときに通信ネットワーク170を介して認証局証明書管理サーバ180から入手し、電子身分証明書認証局証明書182を検定することができる。

【0162】これにより、電子身分証明書確認装置1200は、全ての電子身分証明書認証局203の電子身分証明書認証局証明書182を予め認証局証明書/CRL格納ディスク128に格納しておく必要がなくなり、認証局証明書/CRL格納ディスク128の所要量や、電子身分証明書確認装置1200の管理者が電子身分証明書認証局証明書182を入手する手間を低減することができる。

【0163】例えば電子身分証明書確認装置1200の認証局証明書/CRL格納ディスク128には確認する頻度の高い電子身分証明書認証局203の電子身分証明書認証局証明書182を格納しておき、その他の電子身分証明書認証局203の電子身分証明書認証局証明書182は、電子身分証明書認証局203が発行した電子身分証明書100を確認する必要が発生したときに、認証局証明書管理サーバ180から電子身分証明書認証局証明書182を入手する様にすることができる。

【0164】この様にしても、本実施形態によれば、電子身分証明書確認装置1200が電子身分証明書認証局証明書182を入手した際に、電子身分証明書認証局証

明書182を検定することにより、電子身分証明書認証局203の権威が保証されていることを簡単に確認することができる。

【0165】また、電子身分証明書認証局証明書182を検定することにより、電子身分証明書認証局証明書182及びそれが含む電子身分証明書認証局公開鍵1823が偽造されたことを検出できるので、電子身分証明書100が偽造されていることを検出できる。

【0166】また、本実施形態によれば、電子身分証明書確認装置1200はCRL184を通信ネットワーク170を介して認証局証明書管理サーバ180から入手することができるので、電子身分証明書確認装置1200の管理者がCRL184を入手する手間を低減できる。

【0167】以上説明した様に本実施形態の電子データ処理システムによれば、電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【0168】(実施形態3)以下に所有者の身体的特徴を示す身体情報及びその電子署名を有する電子身分証明書の発行を行う実施形態3の電子データ処理システムについて説明する。

【0169】実施形態3は、電子身分証明書100の発行装置の動作を説明する為のものであり、電子身分証明書100を作成する手順を説明するものである。図15及び図16を用いて本実施形態を説明する。先ず図15を用いて電子身分証明書100の発行装置の構造について説明する。

【0170】図15は本実施形態の電子身分証明書発行装置の概略構成を示す図である。図15に示す様に本実施形態の電子身分証明書発行装置1220は、電子身分証明書入出力部1241と、電子身分証明書情報入力部1242と、身体情報入力部1243と、電子署名作成部1244と、電子身分証明書作成部1245とを有している。

【0171】電子身分証明書入出力部1241は記憶媒体入出力デバイス121を介して電子身分証明書記憶媒体110との間で入出力処理を行って、電子身分証明書作成部1245により作成された電子身分証明書100を電子身分証明書記憶媒体110に書き込む処理部である。

【0172】電子身分証明書情報入力部1242は電子身分証明書情報101の身分情報1013を入力する処理部である。身体情報入力部1243は身体情報入力デバイス122を介して電子身分証明書情報101の所有者の身体情報102を読み取る処理部である。

【0173】電子署名作成部1244は電子身分証明書情報101及び身体情報102に対する電子身分証明書認証局電子署名103を作成する処理部である。電子身

分証明書作成部 1245 は電子身分証明書情報 101、電子身分証明書情報 101 の所有者の身体情報 102 及びその電子身分証明書認証局電子署名 103 を有する電子身分証明書 100 を作成する処理部である。

【0174】電子身分証明書発行装置 1220 を電子身分証明書入出力部 1241、電子身分証明書情報入力部 1242、身体情報入力部 1243、電子署名作成部 1244 及び電子身分証明書作成部 1245 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体は CD-ROM 以外の他の媒体でも良い。

【0175】本実施形態において、電子身分証明書発行装置 1220 は、電子身分証明書認証局 203 に設置される。電子身分証明書発行装置 1220 には、電子身分証明書認証局ディスク 205 が接続される。

【0176】電子身分証明書発行装置 1220 は、メモリ 130 に電子身分証明書発行部 1240 と認証局秘密鍵管理部 1250 なるプログラムを持つ。その他、電子身分証明書確認装置 120 と同様に、記憶媒体入出力デバイス 121、身体情報入力デバイス 122、ディスプレイ 123、CPU 124、キーボード 125、マウス 126 を有する。

【0177】電子身分証明書発行部 1240 は、電子身分証明書 100 の申請者の電子身分証明書 100 を作成する。認証局秘密鍵管理部 1250 は、電子身分証明書 100 の電子身分証明書認証局電子署名 103 を作成する為に用いる電子身分証明書認証局秘密鍵 204 を電子身分証明書認証局ディスク 205 から検索する。

【0178】次に図 16 を用いて、電子身分証明書発行部 1240 の処理を説明する。なお本実施形態では、図 16 の動作の事前に、電子身分証明書認証局 203 が申請者が電子身分証明書 100 を所有するに足る資格を有しているかどうかの審査を終え、電子身分証明書 100 の発行を認定しているものとする。

【0179】図 16 は本実施形態の電子身分証明書発行部 1240 の処理手順を示すフローチャートである。図 16 で先ず電子身分証明書 100 の申請者は、電子身分証明書記憶媒体 110 を記憶媒体入出力デバイス 121 に挿入する (1302)。電子身分証明書 100 の申請者が、キーボード 125 を介して電子身分証明書記憶媒体 110 の暗証番号 112a を入力する (1304) と、電子身分証明書入出力部 1241 は入力された暗証番号 112a と暗証番号 112 を比較する (1306)。

【0180】暗証番号 112a と暗証番号 112 とが一致しなければ、電子身分証明書 100 の発行はできずに終了する。一致すれば、電子身分証明書 100 の申請者はキーボード 125 またはマウス 126 を用いて電子身分証明書情報 101 の身分情報 1013 の為の情報を入

力する (1308)。本実施形態において、この手順は電子身分証明書 100 の発行者が行っても良い。

【0181】次に電子身分証明書発行部 1240 の電子身分証明書情報入力部 1242 は、入力された情報を受け取り、身分情報 1013 を作成する (1310)。

【0182】電子身分証明書 100 の申請者は、身体情報入力デバイス 122 を用いて身体情報 102 の為の情報を入力し (1312)、身体情報入力部 1243 は、入力された情報を受け取り身体情報 102 を作成する (1314)。

【0183】電子身分証明書作成部 1245 は、電子身分証明書情報 101 の電子身分証明書 ID 1011 を決定し、自らの電子身分証明書認証局証明書 182 の認証局証明書 ID 1821 を調べ、電子身分証明書情報 101 を作成する (1316)。

【0184】電子署名作成部 1244 は、認証局秘密鍵管理部 1250 を介して、自らの電子身分証明書認証局秘密鍵 204 を電子身分証明書認証局ディスク 205 から読み込む (1318)。

【0185】次に電子署名作成部 1244 は、電子身分証明書情報 101 と身体情報 102 を電子署名対象データ 501 として、電子身分証明書認証局秘密鍵 204 を用いて電子身分証明書認証局電子署名 103 を作成する (1320)。

【0186】電子身分証明書作成部 1245 は、電子身分証明書情報 101、身体情報 102、電子身分証明書認証局電子署名 103 により、電子身分証明書 100 を作成する (1322)。電子身分証明書入出力部 1241 は、電子身分証明書記憶媒体 110 に電子身分証明書 100 を書き込む (1324)。最後に、電子身分証明書入出力部 1241 は、電子身分証明書一覧 111 に、当該電子身分証明書のエントリを追加する (1326)。

【0187】この様に本実施形態によれば、電子データとして実現した身分証明書であり、身体情報 102 と身体情報 102 に対する電子身分証明書認証局電子署名 103 を有する電子身分証明書 100 を作成することができる。

【0188】(実施形態 4) 以下に所有者の身体的特徴を示す身体情報を圧縮・復元する実施形態 4 の電子データ処理システムについて説明する。

【0189】実施形態 1 では、電子身分証明書 100 の身体情報 102 は、当該電子身分証明書の所有者の身体的特徴を示すデータそのものであった。本実施形態では、身体情報 102 を、当該電子身分証明書の所有者の身体的特徴を示すデータを圧縮したデータとする。

【0190】本実施形態では、電子身分証明書発行装置 1220 は、電子身分証明書 100 の申請者が入力した身体情報を圧縮し、身体情報 102 に変換する処理部を有する。また電子身分証明書確認装置 120 は、電子身

分証明書100の身体情報102を圧縮前の身体情報に復元する処理部を有する。

【0191】この様に本実施形態によれば、電子身分証明書100のサイズを低減することができる。

【0192】（実施形態5）以下に所有者の身分情報を暗号化する実施形態5の電子データ処理システムについて説明する。

【0193】実施形態1では、電子身分証明書100の身分情報1013は暗号化されていない。本実施形態では、身分情報1013を暗号化された電子データとする。

【0194】本実施形態では、電子身分証明書発行装置1220の電子身分証明書認証局ディスク205に身分情報1013を暗号化する為の暗号鍵を格納し、電子身分証明書発行装置1220が身分情報1013を暗号化する処理部を備える。

【0195】また、電子身分証明書確認装置120の認証局証明書/CRL格納ディスクに身分情報1013を復号する為の暗号鍵を格納し、電子身分証明書確認装置120が身分情報1013を復号する処理部を備える。

【0196】電子身分証明書確認装置120は、予め、身分情報1013を復号する為の暗号鍵を入手しておく。例えば統括認証局公開鍵183を入手する際に入手する。本実施形態では、身分情報1013を暗号化するとしたが、同様に、身体情報102を暗号化することもできる。

【0197】この様に本実施形態によれば、電子身分証明書100の中の身分情報1013や身体情報102を秘匿することができる。

【0198】（実施形態6）以下に任意の情報及びその電子署名を追加する実施形態6の電子データ処理システムについて説明する。

【0199】本実施形態の電子身分証明書は、電子身分証明書の発行後に、当該電子身分証明書に任意の情報を追加できる様にし、かつ、追加した情報が確かであることを保証するものである。図17及び図18を用いて本実施形態を説明する。

【0200】図17は本実施形態の電子身分証明書の構造を示す図である。電子身分証明書1700は、実施形態1の電子身分証明書100と同様に、電子身分証明書情報101、身体情報102、電子身分証明書認証局電子署名103を有すると共に、追加情報証明書1702なる電子データを含む。

【0201】追加情報証明書1702は、電子身分証明書1700の確認を行った際に電子身分証明書1700へ追加する情報を保持し、かつ、その内容を保証する為の電子データである。

【0202】追加情報証明書1702は、認証局証明書ID1012、追加情報1704、追加情報認証局電子署名1706から構成される。

【0203】追加情報1704は、電子身分証明書情報101の発行機関である電子身分証明書認証局203とは別の機関が作成した任意の情報であり、電子身分証明書1700の確認を行った際に電子身分証明書1700へ追加される情報である。追加情報認証局電子署名1706は、追加情報1704を電子身分証明書1700に追加する機関の秘密鍵によって作成される電子署名であり、追加情報1704を対象データとする電子署名である。認証局証明書ID1012は、追加情報1704を電子身分証明書1700に追加する機関の暗号鍵証明書の一意な番号である。

【0204】本実施形態では、実施形態1の電子身分証明書確認装置120が設置される機関に、図18の追加情報証明書発行装置が設置されているとする。本実施形態では、このような機関を追加情報認証局と呼ぶ。図18を用いて、追加情報証明書発行装置の構造と動作を説明する。

【0205】図18は本実施形態の追加情報証明書発行装置の概略構成を示す図である。図18に示す様に本実施形態の追加情報証明書発行装置1920は、追加情報証明書入出力部1941と、追加情報証明書情報入力部1942と、電子署名作成部1944と、追加情報証明書作成部1945とを有している。

【0206】追加情報証明書入出力部1941は電子身分証明書1700に追加情報証明書1702を追加し電子身分証明書記憶媒体110に書き込む処理部である。追加情報証明書情報入力部1942はキーボード125やマウス126を介して入力される追加情報1704を受け取る処理部である。

【0207】電子署名作成部1944は追加情報1704に対する追加情報認証局電子署名1706を追加情報認証局秘密鍵1961により作成する処理部である。追加情報証明書作成部1945は追加情報認証局証明書1962の一意な番号と追加情報1704と作成した追加情報認証局電子署名1706を複合して追加情報証明書1702を作成する処理部である。

【0208】追加情報証明書発行装置1920を追加情報証明書入出力部1941、追加情報証明書情報入力部1942、電子署名作成部1944及び追加情報証明書作成部1945として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はCD-ROM以外の他の媒体でも良い。

【0209】追加情報証明書発行装置1920は、電子身分証明書確認装置120や電子身分証明書発行装置1220と同様に、記憶媒体入出力デバイス121、身体情報入力デバイス122、メモリ130、ディスプレイ123、CPU124、キーボード125、マウス12

6、バス127を備える。



【0210】また、メモリ 130 には、追加情報証明書発行部 1940 と認証局秘密鍵管理部 1950 というプログラムが存在する。また、追加情報認証局ディスク 1960 を備え、追加情報認証局ディスク 1960 には追加情報認証局秘密鍵 1961 と追加情報認証局証明書 1962 が格納されている。

【0211】追加情報認証局証明書 1962 は、追加情報認証局秘密鍵 1961 と暗号鍵ペアを成す公開鍵の暗号鍵証明書である。追加情報認証局証明書 1962 は、実施形態 1 の統括認証局 200 と同様の機関から発行され、実施形態 2 の認証局証明書管理サーバ 180 と同様の機関に渡され保管されるとする。追加情報証明書発行部 1940 は、以下の様に動作する。

【0212】追加情報証明書情報入力部 1942 はキーボード 125 やマウス 126 を介して入力される追加情報 1704 を受け取り、電子署名作成部 1944 は追加情報 1704 に対する追加情報認証局電子署名 1706 を追加情報認証局秘密鍵 1961 により作成する。

【0213】追加情報証明書作成部 1945 は追加情報認証局証明書 1962 の一意な番号と追加情報 1704 と作成した追加情報認証局電子署名 1706 を複合して追加情報証明書 1702 を作成し、追加情報証明書入出力部 1941 が電子身分証明書 1700 に追加情報証明書 1702 を追加し電子身分証明書記憶媒体 110 に書き込む。本実施形態では、追加情報 1704 にその発行機関の電子署名を施すことにより、追加情報 1704 の内容が確かであることを保証する。

【0214】本実施形態において、電子身分証明書 1700 は、例えばパスポートである。この場合、追加情報 1704 は、例えば出国審査の証明情報であり、追加情報認証局電子署名 1706 は、例えば出国審査の証明印であると考えることができる。ここでは、出国審査機関を追加情報認証局と考えることができる。

【0215】出国審査機関には、電子身分証明書確認装置 120 と追加情報証明書発行装置 1920 が設置される。出国審査機関は、審査の申請者のパスポートである電子身分証明書 1700 を実施形態 1 と同様に電子身分証明書確認装置 120 により確認した後、追加情報証明書発行装置 1920 により追加情報証明書 1702 を作成し、電子身分証明書 1700 に追加する。

【0216】後で、他の機関が当該追加情報を確認する必要がある場合には、当該機関は、追加情報証明書 1702 の追加情報認証局電子署名 1706 を検定する。この検定操作に必要な追加情報認証局証明書 1962 は、実施形態 1 の認証局証明書管理サーバ 180 に類する機関から取得することができる。

【0217】この様に本実施形態によれば、電子身分証明書 1700 が様々な機関により確認されるたびに、当該機関が内容を保証する情報を当該電子身分証明書 1700 に追加し、後ほど電子身分証明書 1700 の所有者

が当該機関により保証される内容の情報を授与されているかを確認することができる。

【0218】（実施形態 7）以下に電子身分証明書の身体情報を別構造として記憶する実施形態 7 の電子データ記録媒体について説明する。

【0219】図 19 は本実施形態の電子身分証明書及びその記憶媒体の概要を示す図である。本実施形態の電子身分証明書 2000 は、電子身分証明書情報 101 と電子身分証明書認証局電子署名 2002 から構成される。

10 電子身分証明書 2000 は、実施形態 1 の電子身分証明書 100 と異なり、身体情報 102 を含まない。また電子身分証明書認証局電子署名 2002 は、電子身分証明書情報 101 を対象データとする電子署名である。

【0220】一方本実施形態では、身体情報証明書 2020 を設ける。身体情報証明書 2020 は、身体情報 102 を含む電子データであり、身体情報 102 の内容を保証する為の電子データである。身体情報証明書 2020 は、実施形態 1 の電子身分証明書認証局 203 のいずれかが発行するものである。

20 【0221】身体情報証明書 2020 は、身体情報証明書情報 2021、身体情報認証局電子署名 2023 から構成される。身体情報証明書情報 2021 は、身体情報証明書 ID 2022、認証局証明書 ID 1012、身体情報 102 から構成される。身体情報認証局電子署名 2023 は、身体情報証明書情報 2021 を対象データとする電子署名であり、実施形態 1 の電子身分証明書認証局 203 のいずれかが作成する。

30 【0222】身体情報証明書 ID 2022 は、当該身体情報証明書の一意な番号である。認証局証明書 ID 1012 は、身体情報認証局電子署名 2023 を作成した電子身分証明書認証局 203 の電子身分証明書認証局証明書 182 の一意な番号である。

40 【0223】本実施形態において、電子身分証明書記憶媒体 2010 は、電子身分証明書 2000 を格納する記憶媒体である。電子身分証明書記憶媒体 2010 は、実施形態 1 の電子身分証明書記憶媒体 110 と同様に電子身分証明書一覧 111、暗証番号 112 を格納する。また電子身分証明書記憶媒体 2010 は、身体情報証明書 2020 と電子身分証明書 2000 を格納する。電子身分証明書記憶媒体 2010 は、単一の身体情報証明書 2020 と、複数の電子身分証明書 2000 を格納する。

【0224】本実施形態では、電子身分証明書 2000 を確認する為の装置は、実施形態 1 の電子身分証明書確認装置 120 と同様の構成を有する。但し、本実施形態において、電子身分証明書検定部 140 の電子署名検定部 144 は、電子身分証明書認証局電子署名 2002 の検定と、身体情報認証局電子署名 2023 の検定を行う。身体情報検定部 146 は、身体情報証明書 2020 に入っている身体情報 102 を用いて、入力された身体情報 102 a を検査する。

【0225】この様に本実施形態によれば、身体情報102が電子身分証明書2000には含まれないので、電子身分証明書2000のサイズを実施形態1の電子身分証明書100に比べて低減できる。

#### 【0226】

【発明の効果】本発明によれば電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

#### 【図面の簡単な説明】

【図1】実施形態1の電子身分証明書のデータ構造、電子身分証明書を記憶する記憶媒体及び電子身分証明書確認装置の概略構成を示す図である。

【図2】実施形態1の電子データ処理システムのシステム構成を示す図である。

【図3】実施形態1の電子身分証明書認証局203の概念を示す図である。

【図4】実施形態1の電子身分証明書100、電子身分証明書認証局証明書182及びCRL184のデータ構造を示す図である。

【図5】実施形態1の電子身分証明書100の作成の原理を示す図である。

【図6】実施形態1の電子身分証明書100の確認の原理を示す図である。

【図7】実施形態1の電子身分証明書認証局証明書182の確認の原理を示す図である。

【図8】実施形態1の電子身分証明書一覧111の概要を示す図である。

【図9】実施形態1の電子身分証明書確認装置120が電子身分証明書100の確認を行う処理の処理手順を示すフローチャートである。

【図10】実施形態1の電子身分証明書100の確認装置の動作の内、電子身分証明書100の電子身分証明書認証局電子署名103の検定処理の処理手順を示すフローチャートである。

【図11】実施形態1の電子身分証明書確認装置120が電子身分証明書認証局証明書182とCRL184を入力する処理の処理手順を示すフローチャートである。

【図12】実施形態2の電子身分証明書100のデータ構造、電子身分証明書100を記憶する記憶媒体及びその確認装置の概要を示す図である。

【図13】実施形態2の電子データ処理システムのシステム構成を示す図である。

【図14】実施形態2の電子身分証明書確認装置120の処理手順を示すフローチャートである。

【図15】実施形態3の電子身分証明書発行装置の概略構成を示す図である。

【図16】実施形態3の電子身分証明書発行部1240の処理手順を示すフローチャートである。

【図17】実施形態6の電子身分証明書の構造を示す図である。

【図18】実施形態6の追加情報証明書発行装置の概略構成を示す図である。

【図19】実施形態7の電子身分証明書及びその記憶媒体の概要を示す図である。

#### 【符号の説明】

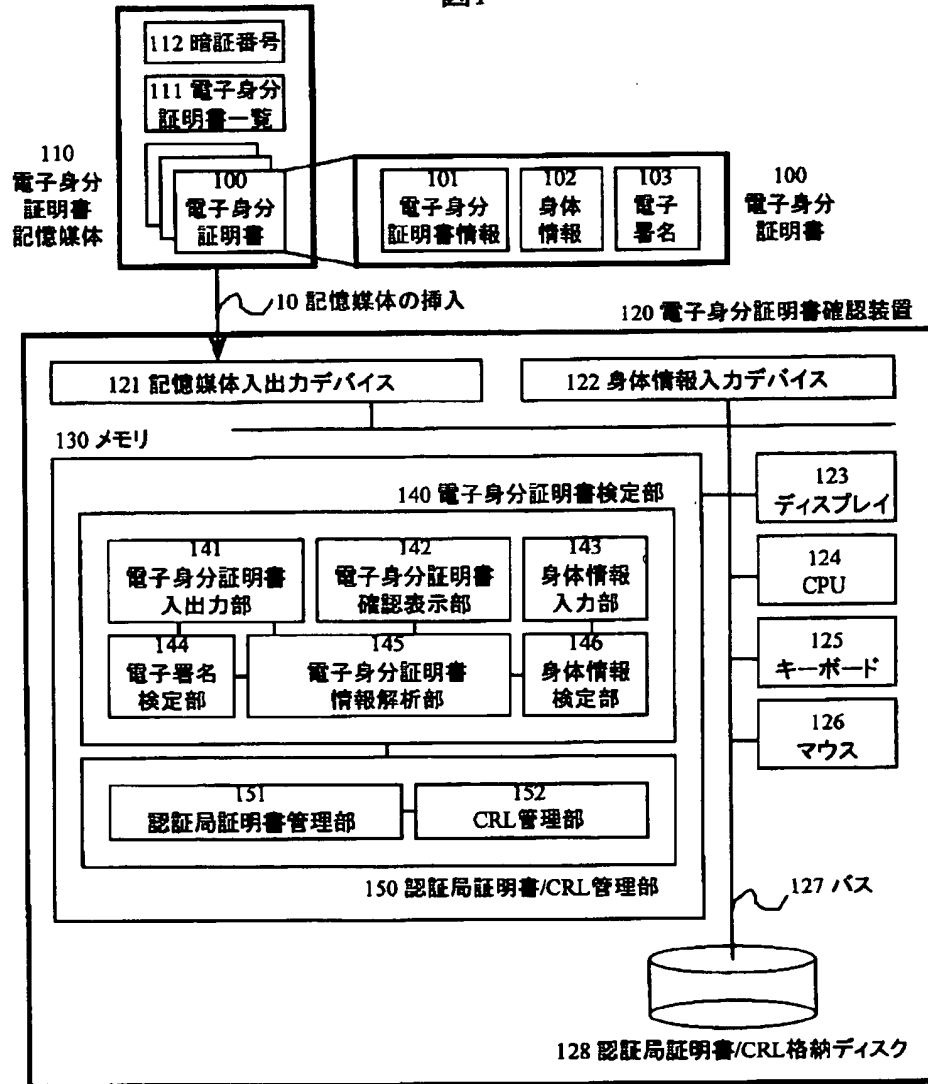
100…電子身分証明書、101…電子身分証明書情報、102…身体情報、103…電子身分証明書認証局電子署名、110…電子身分証明書記憶媒体、111…電子身分証明書一覧、112…暗証番号、120…電子身分証明書確認装置、121…記憶媒体入出力デバイス、122…身体情報入力デバイス、123…ディスプレイ、124…CPU、125…キーボード、126…マウス、127…バス、128…認証局証明書/CRL格納ディスク、130…メモリ、140…電子身分証明書検定部、150…認証局証明書/CRL管理部、141…電子身分証明書入出力部、142…電子身分証明書確認表示部、143…身体情報入力部、144…電子署名検定部、145…電子身分証明書情報解析部、146…身体情報検定部、151…認証局証明書管理部、152…CRL管理部、182…電子身分証明書認証局証明書、183…統括認証局公開鍵、184…CRL、200…統括認証局、201…統括認証局秘密鍵、202…統括認証局ディスク、203…電子身分証明書認証局、204…電子身分証明書認証局秘密鍵、205…電子身分証明書認証局ディスク、311…人物A、312…人物B、1001…運転免許証、1002…パスポート、1003…パスポート、1004…A大学学生証、1101…電子身分証明書記憶媒体A、1102…電子身分証明書記憶媒体B、2031…運転免許証発行機関、2032…パスポート発行機関、2033…A大学学生証発行機関、1011…電子身分証明書ID、1012…認証局証明書ID、1013…身体情報、1821…認証局証明書ID、1823…電子身分証明書認証局公開鍵、1824…統括認証局電子署名、1841…CRLID、1842…電子身分証明書ID、1843…認証局証明書ID、1844…統括認証局電子署名、501…電子署名対象データ、601…電子署名対象データ、701…電子署名対象データ、802…電子身分証明書種別、804…電子身分証明書認証局名、1200…電子身分証明書確認装置、153…認証局証明書管理サーバアクセス部、160…通信ネットワークコントローラ、170…通信ネットワーク、180…認証局証明書管理サーバ、181…認証局証明書管理サーバディスク、1220…電子身分証明書発行装置、1240…電子身分証明書発行部、1250…認証局秘密鍵管理部、1241…電子身分証明書入出力部、1242…電子身分証明書情報入力部、1243…身体情報入力部、1244…電子署名作成部、1245…電子身分証明書作成部、1700…電子身分証明

書、1702…追加情報証明書、1704…追加情報、  
1706…追加情報認証局電子署名、1920…追加情  
報証明書発行装置、1940…追加情報証明書発行部、  
1950…認証局秘密鍵管理部、1960…追加情報認  
証局ディスク、1961…追加情報認証局秘密鍵、19  
62…追加情報認証局証明書、1941…追加情報証明  
書入出力部、1942…追加情報証明書情報入力部、1

944…電子署名作成部、1945…追加情報証明書作  
成部、2000…電子身分証明書、2002…電子身分  
証明書認証局電子署名、2010…電子身分証明書記憶  
媒体、2020…身体情報証明書、2021…身体情報  
証明書情報、2022…身体情報証明書ID、2023…  
身体情報認証局電子署名。

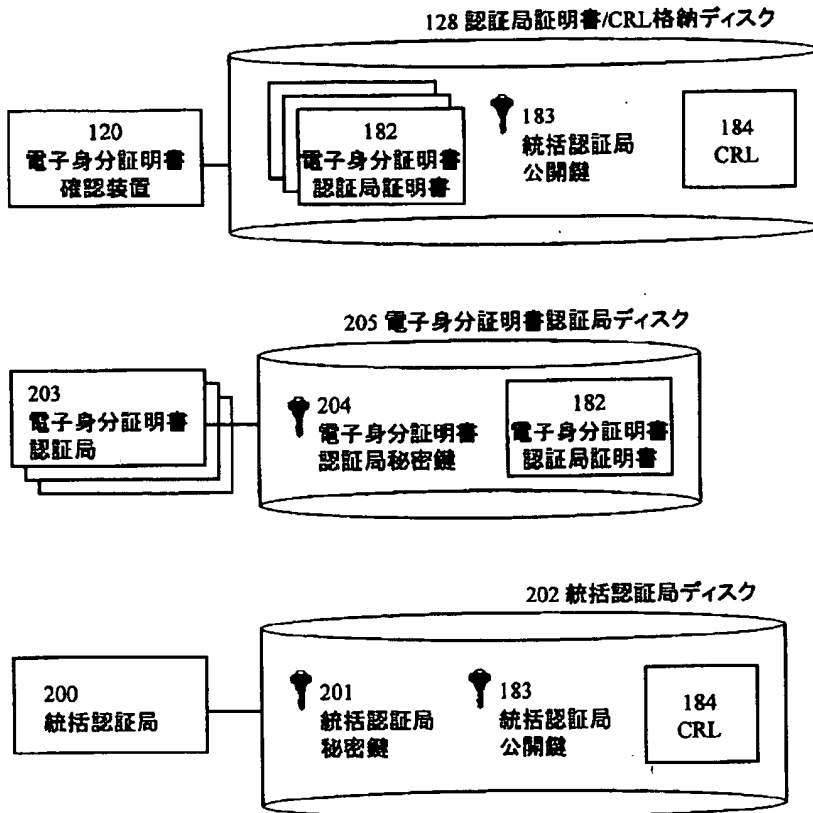
【図1】

図1



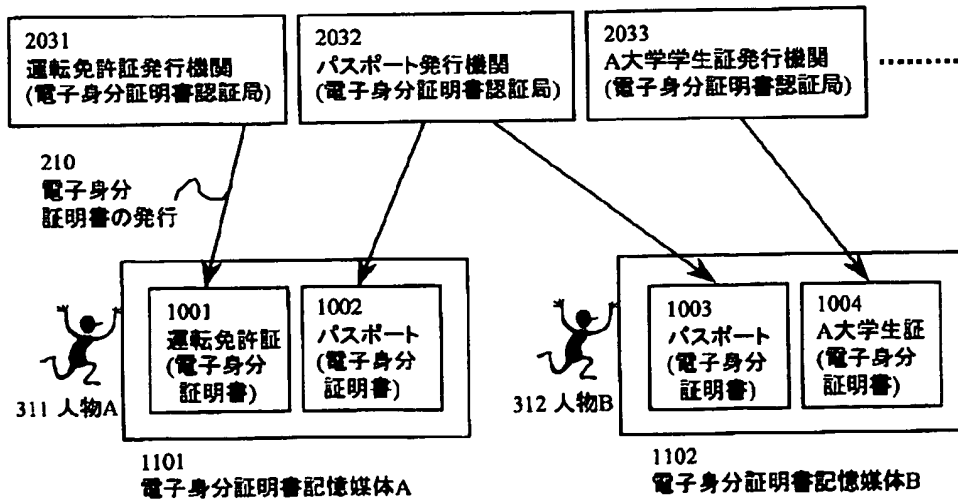
【図2】

図2



【図3】

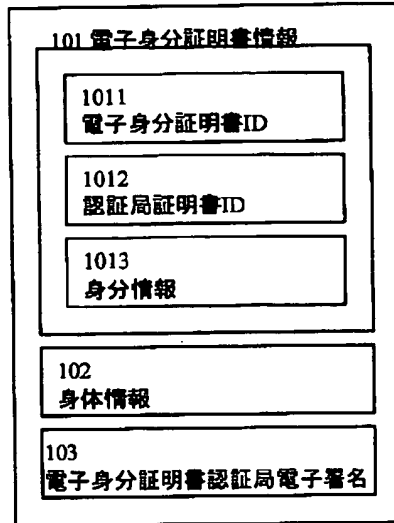
図3



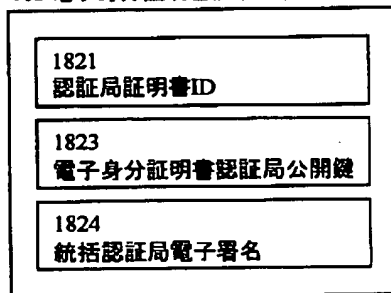
【図 4】

図 4

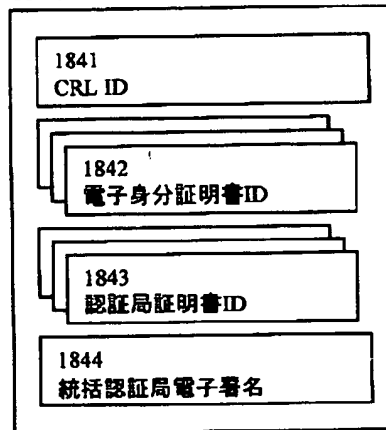
## 100 電子身分証明書



## 182 電子身分証明書認証局証明書



## 184 CRL



【図 8】

図 8

## 111 電子身分証明書一覧

0023199802140232	運転免許証	XXXX
8856199511241923	パスポート	YYYY

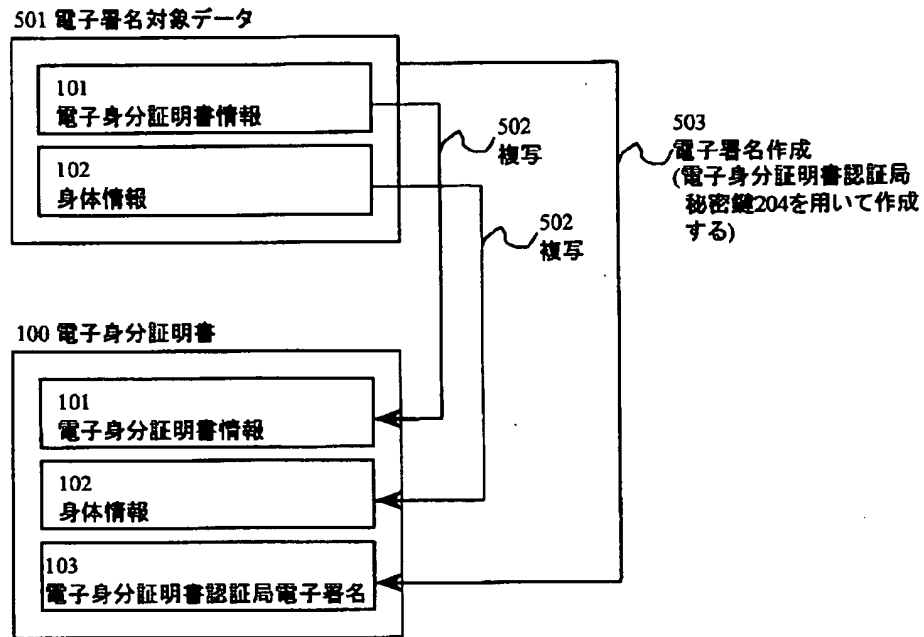
1011  
電子身分証明書ID

802  
電子身分証明書種別

804  
電子身分証明書認証局名

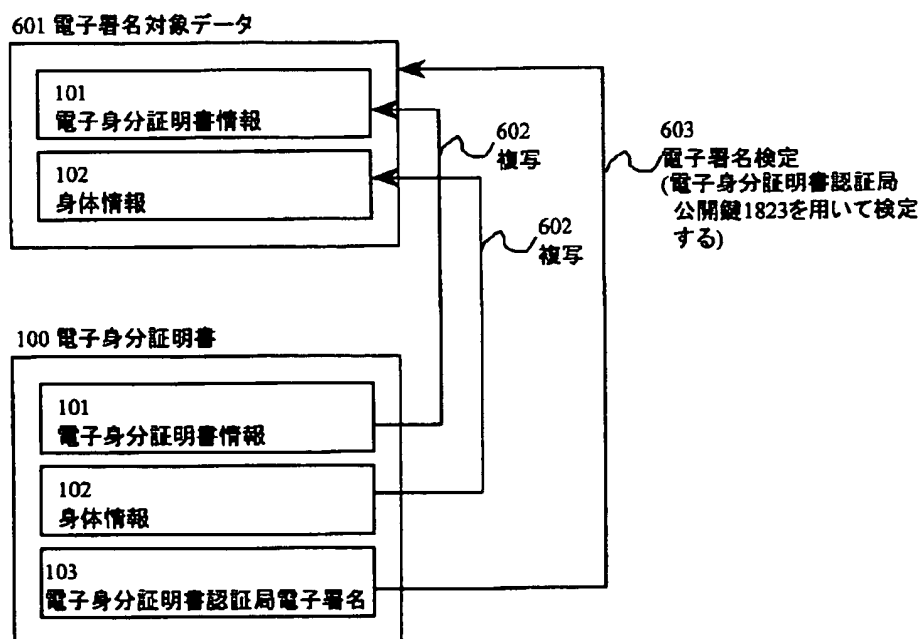
【図5】

図5



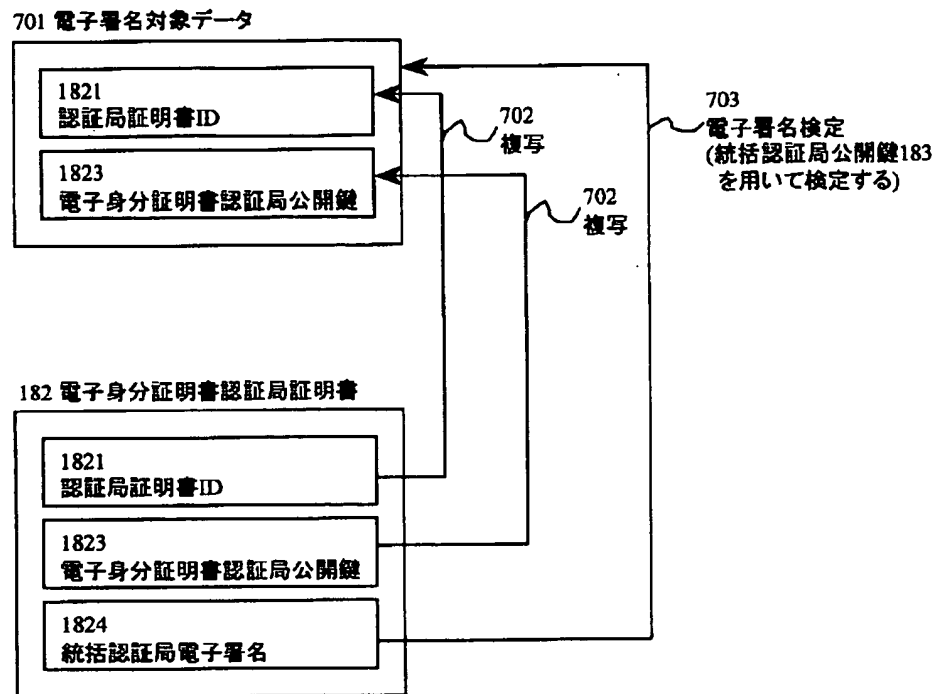
【図6】

図6

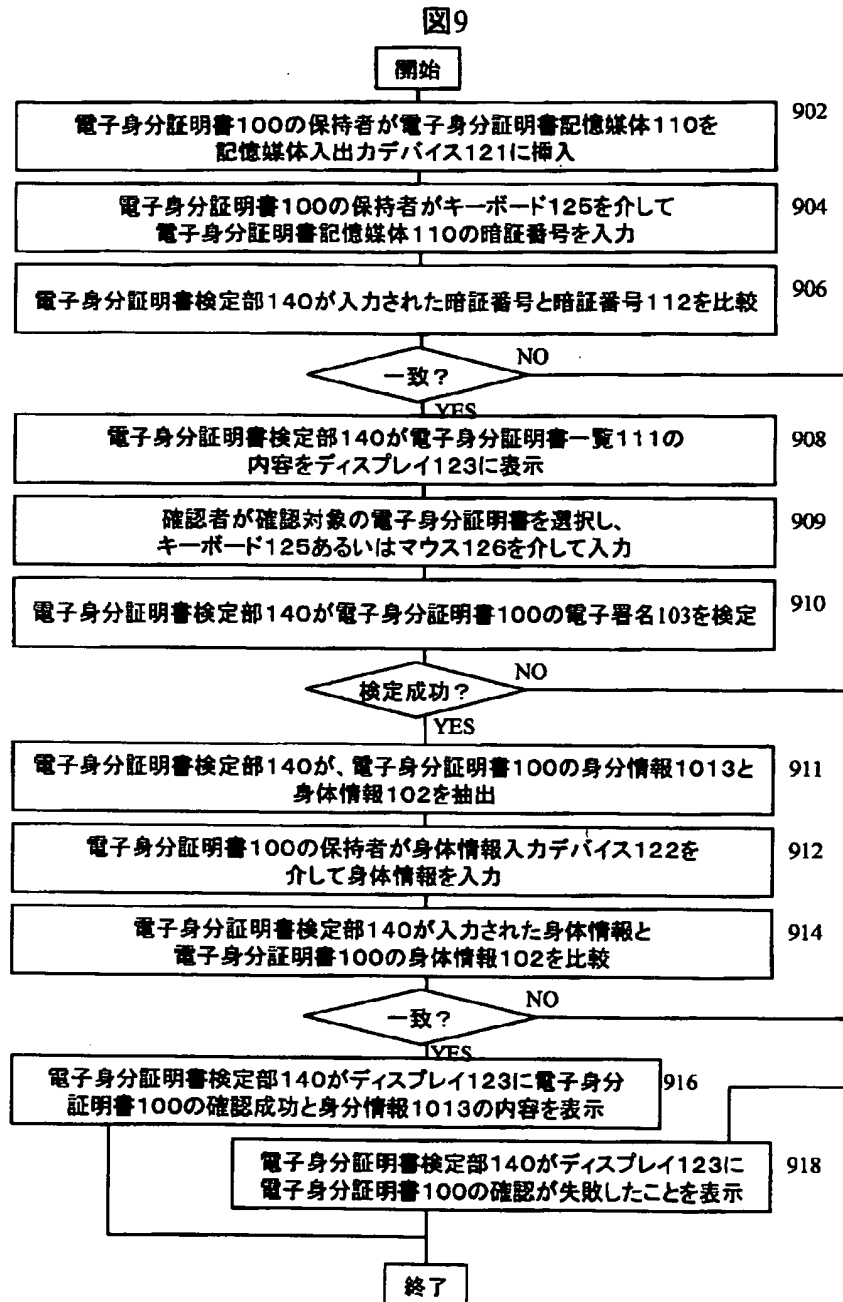


【図7】

図7



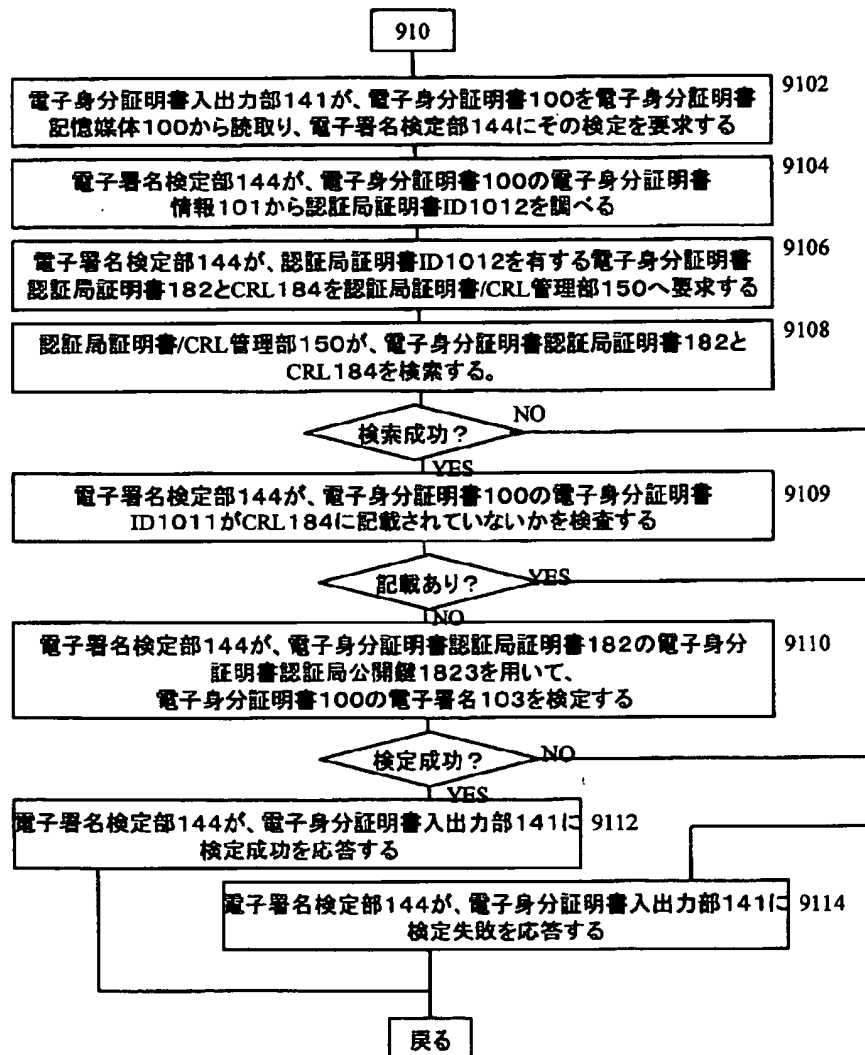
【図9】





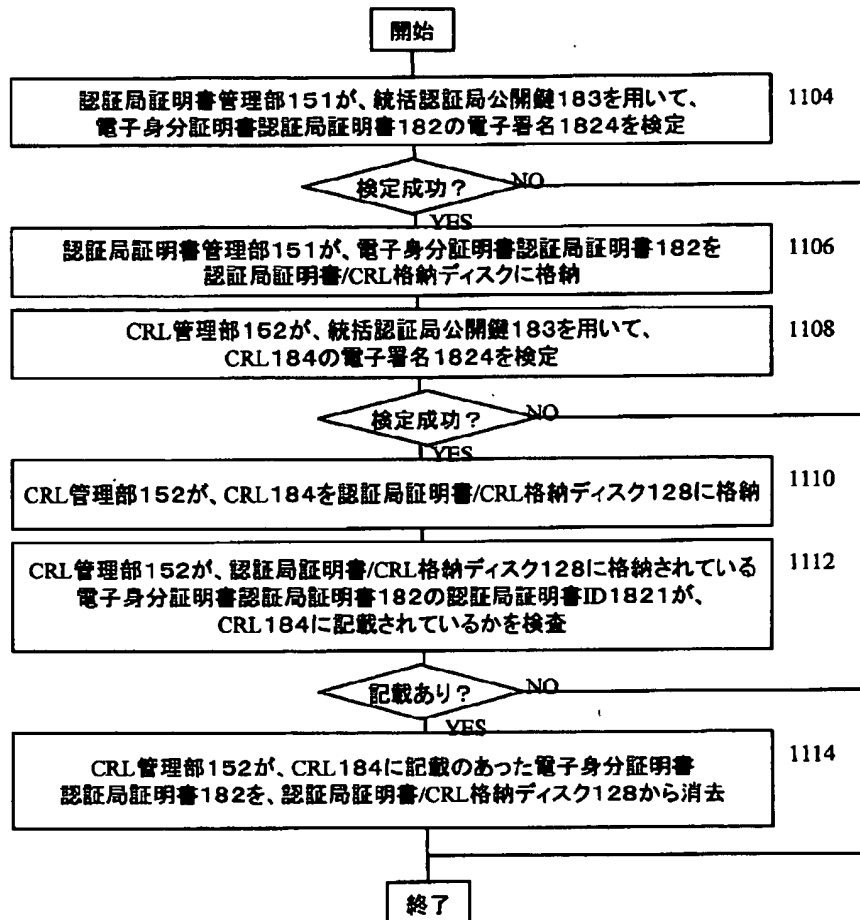
【図 10】

図 10



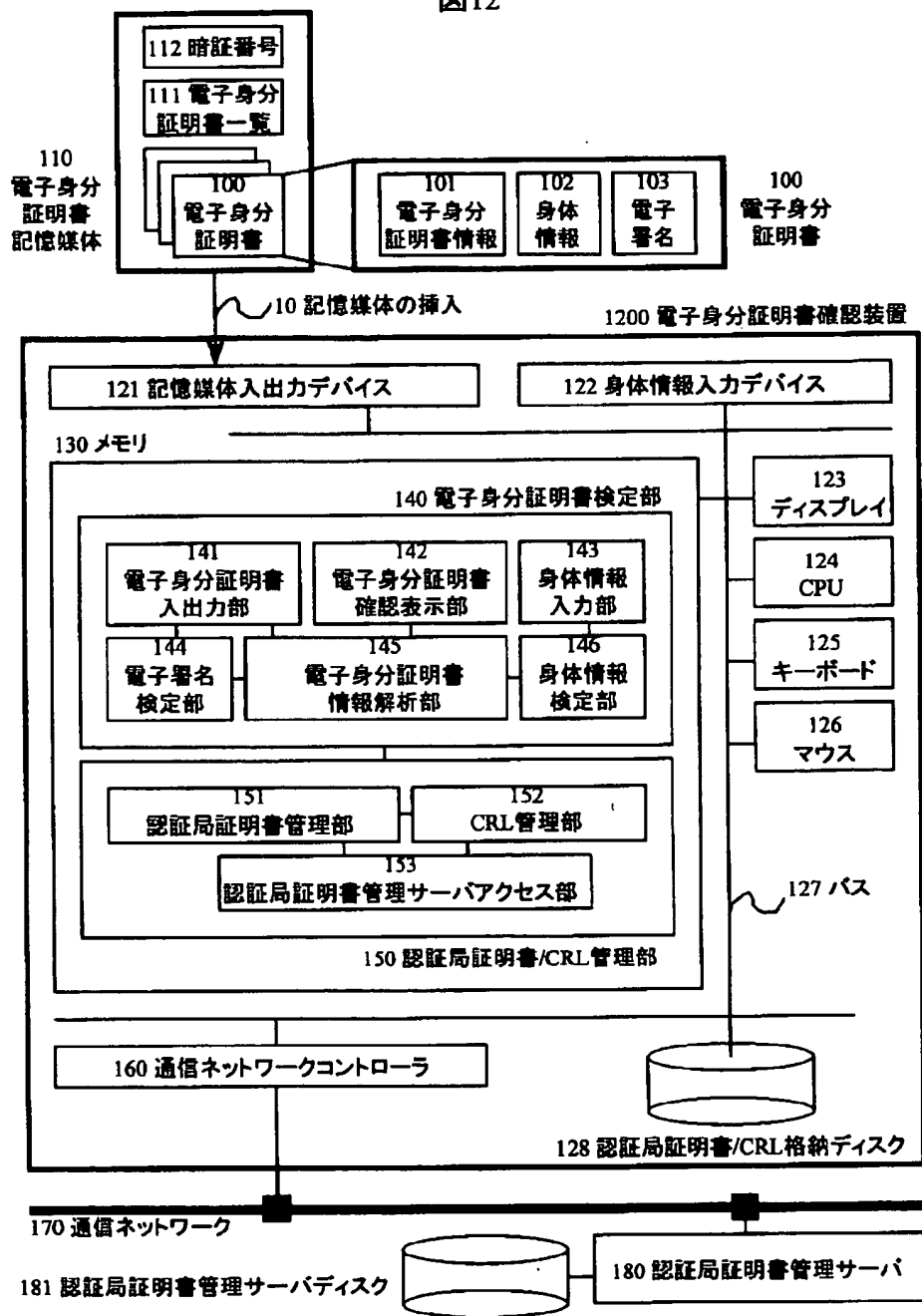
【図11】

図11



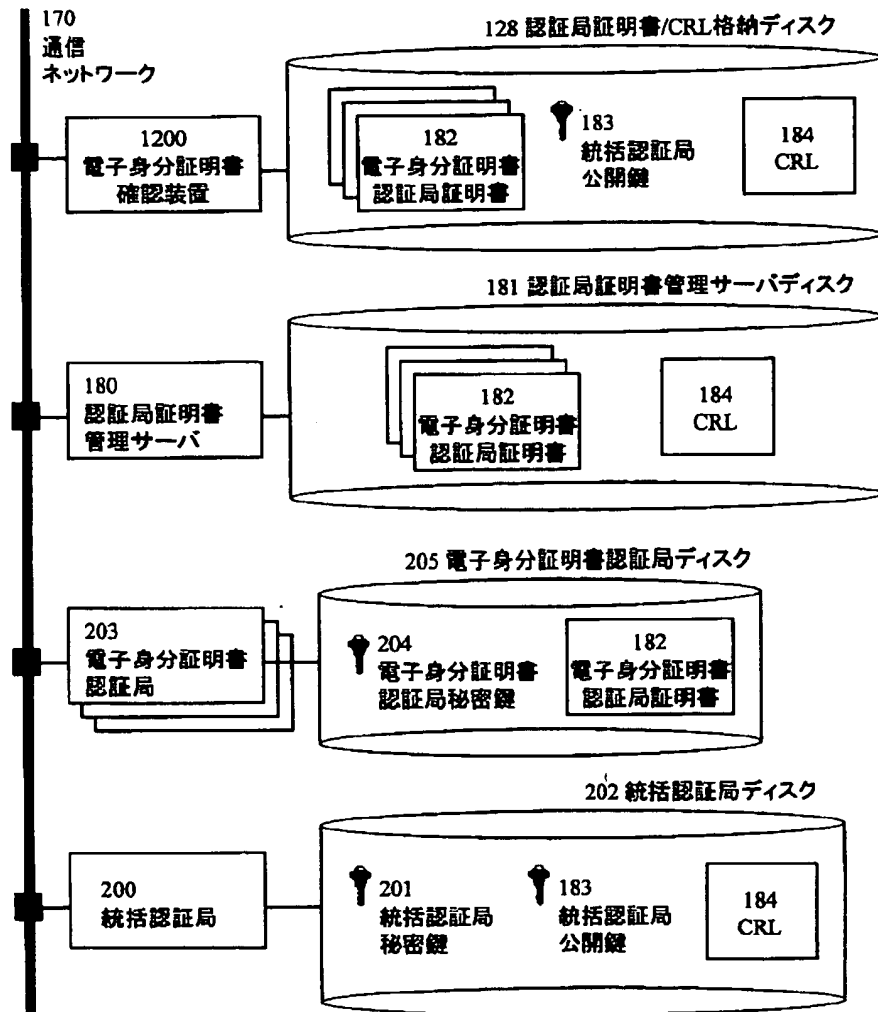
【図 12】

図12

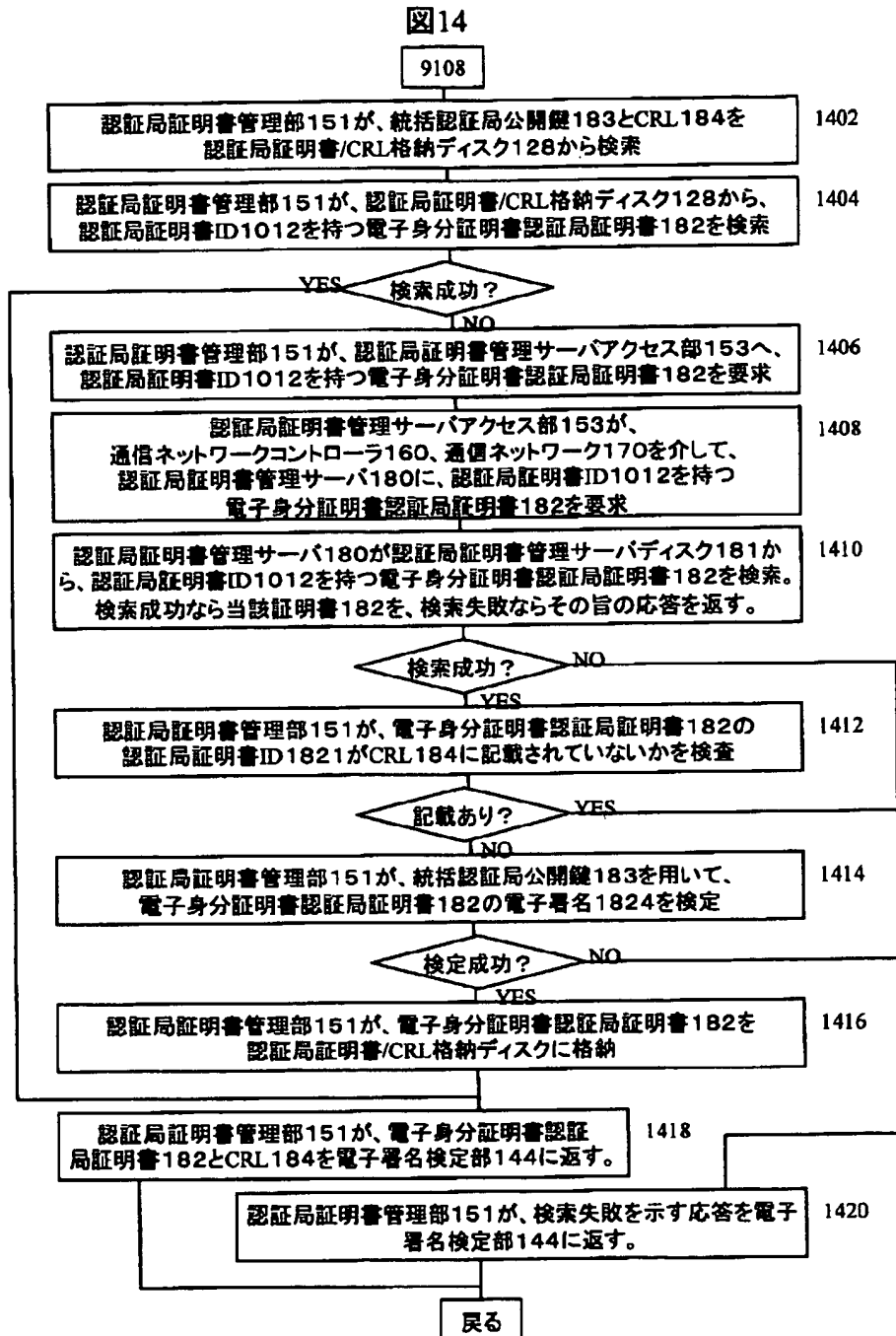


【図13】

図13

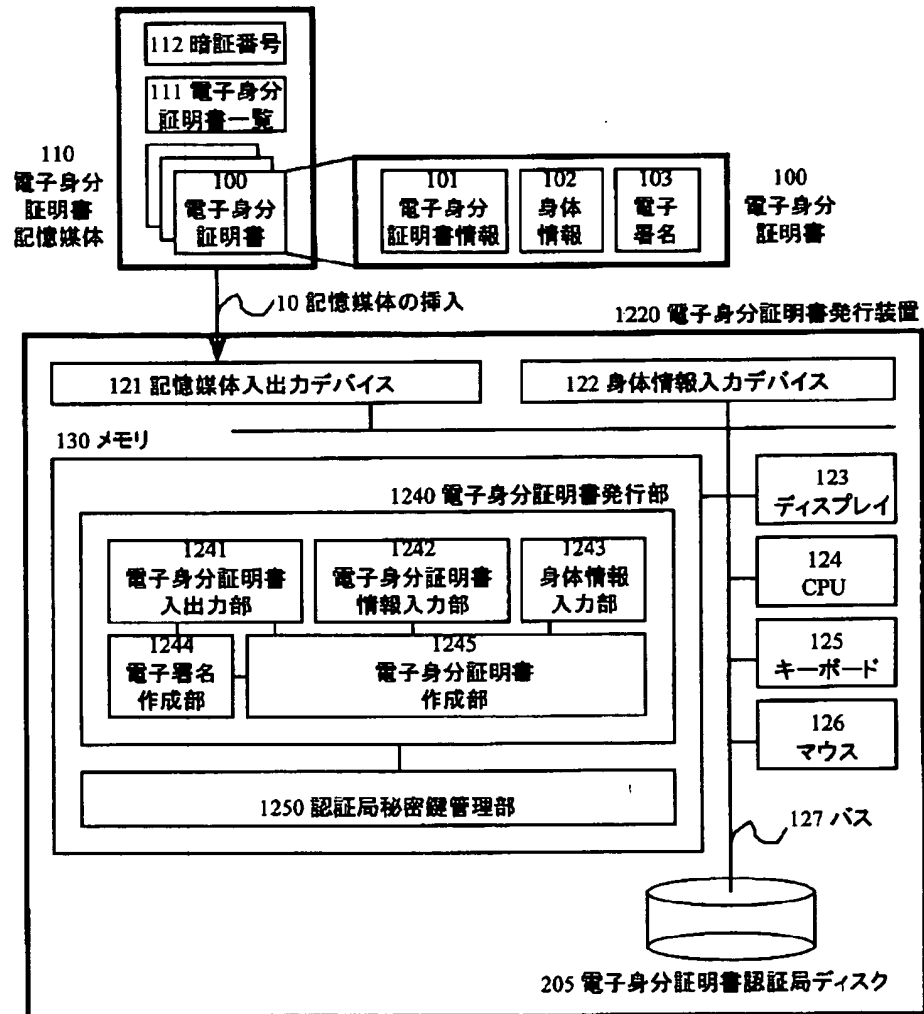


【図14】

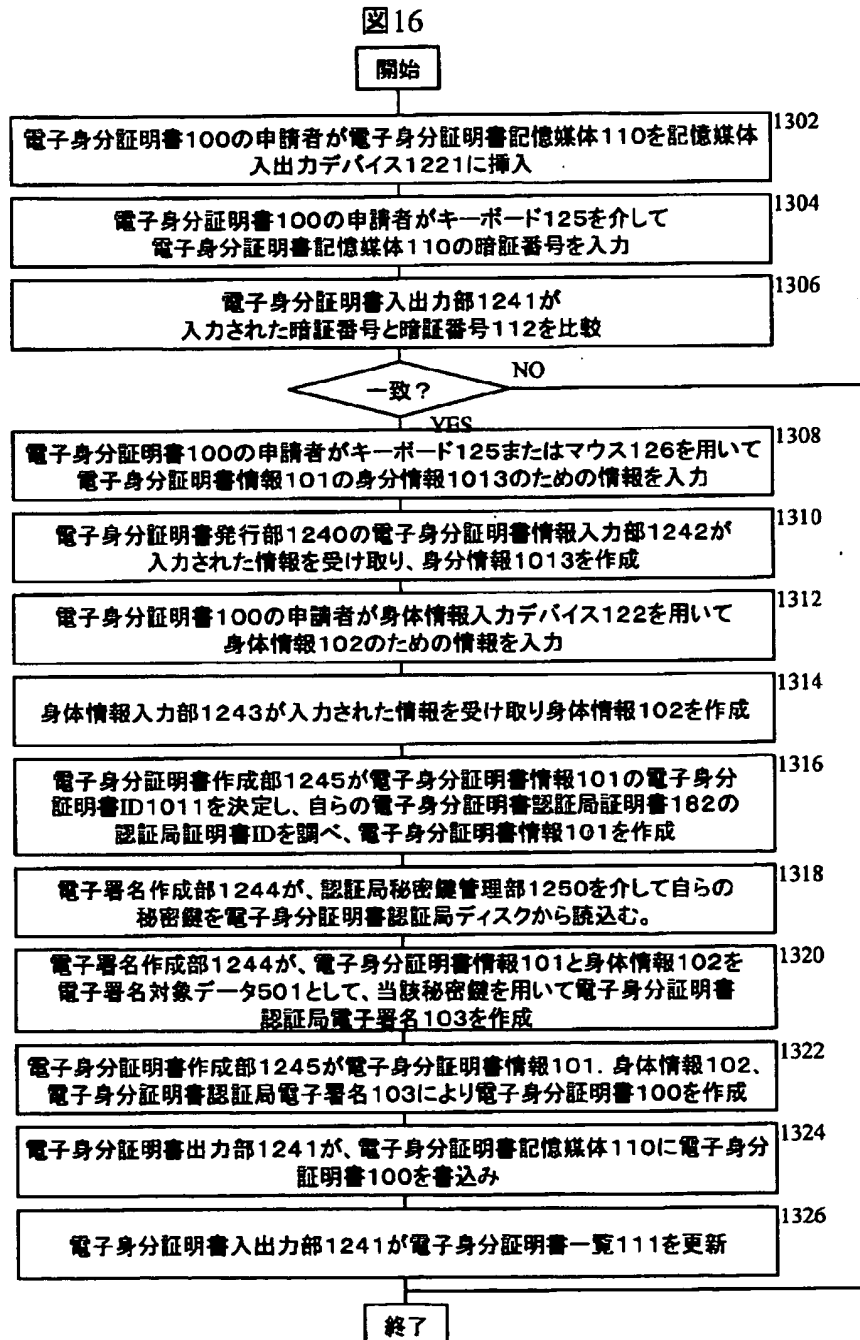


【図15】

図15

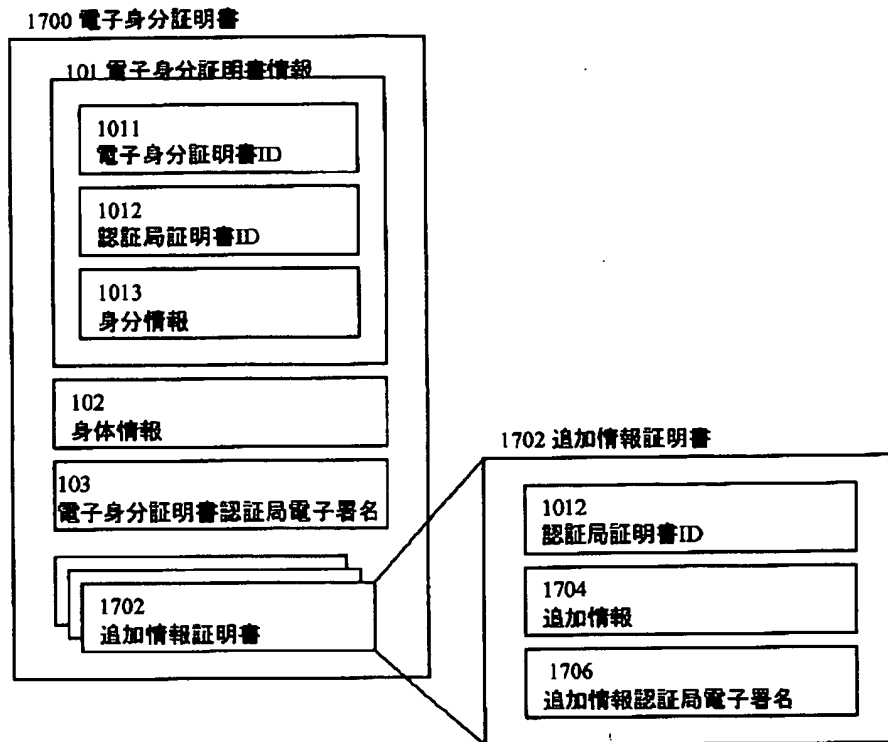


【図 16】



【図17】

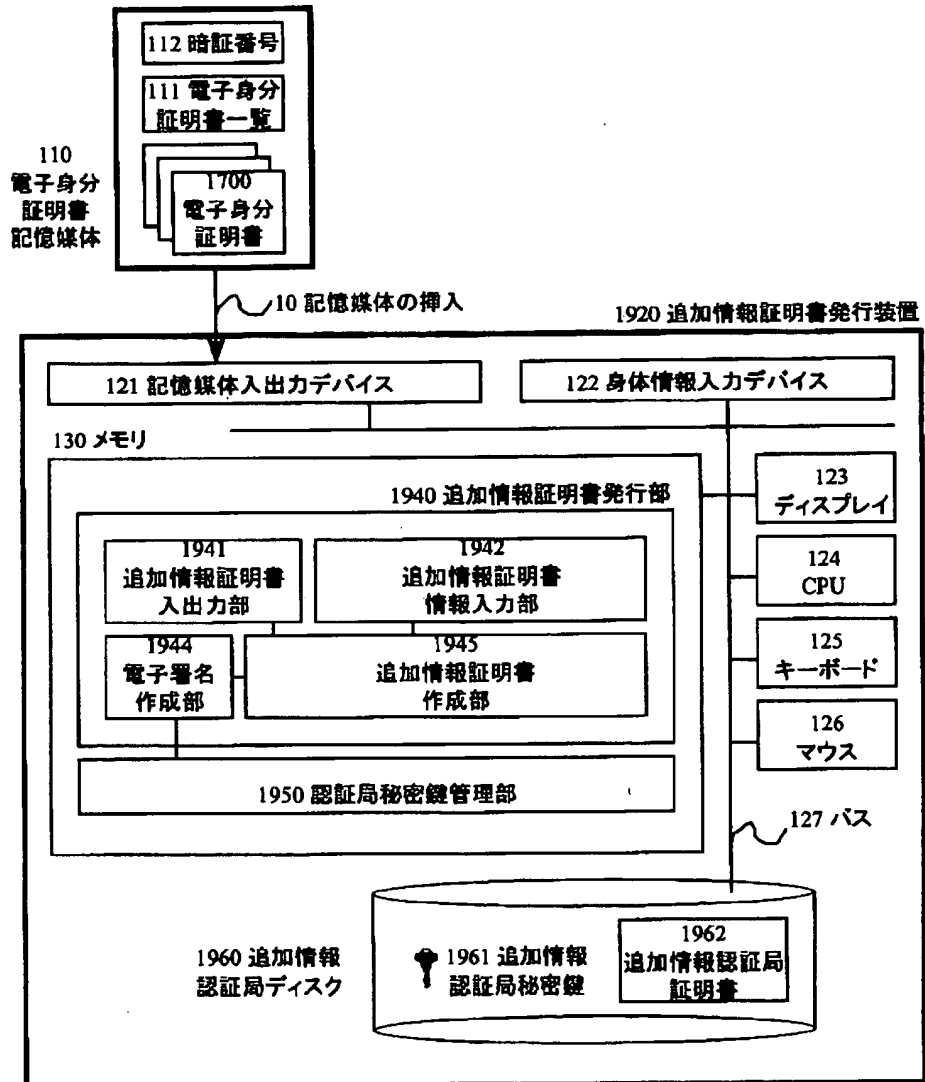
図17





【図18】

図18



【図19】

図19

